Microsoft® Office Groove® Security Architecture

April 2007

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred

Table of Contents

Executive Summary

This paper provides an in-depth technical examination of the Microsoft® Office Groove® 2007 security architecture. The paper is intended for organizations conducting in-depth evaluations of the Office Groove 2007 platform and its potential impact on their existing IT infrastructures.

After reading this paper, you will have a strong understanding of:

- How the Office Groove 2007 security model provides a safe foundation for data storage and communications across Office Groove 2007 environments.
- How the Office Groove 2007 access control model enables enterprises to mirror organizational structures.
- How Office Groove 2007 security policies flexibly support enterprise IT policies inside and outside the firewall.
- How the flexible but strong authentication model enables users to verify identities.
- How organizations can leverage their own Enterprise PKI (public key infrastructure) in the Office Groove 2007 environment or enable application-specific standalone PKI.
- How Office Groove Server 2007 Data Bridge can integrate an organization's business processes securely and seamlessly with Office Groove 2007 workspaces.

As an introduction to Groove 2007 security, this paper begins with a review of current trends in the corporate working environment. Next, it highlights the benefits of the Groove 2007 security model and describes the basic security building blocks of Groove 2007. Then, the paper reviews Groove 2007 security in action — how these building blocks work dynamically to help secure user identities and data within the Groove 2007 environment. Finally, the paper steps back to look at security within a larger context of managed environments, that is, environments in which Office Groove Server 2007 has been deployed or Office Groove Enterprise Services are being utilized.

All the security features described in the paper apply to environments where Office Groove 2007 client software is deployed, unless otherwise noted. Any references to an "on site deployment" indicate that the security features are only available to organizations that have deployed Office Groove Server 2007. Organizations using the hosted Microsoft Office Groove Enterprise Services may not have access to all Groove security features available in an onsite server deployment.

Maintaining Security in the New World of Work

In the past ten years, the work environment has changed dramatically. Conducting business outside the office has become mainstream. The International Telecommuting Association and Council, for example, reports that over 45 million Americans, approximately one in three employees, worked regularly or occasionally from home in 2005. That's a 30% increase in just one year.[1] Employees aren't just limited to their home offices, however. The pervasiveness of wireless networks, along with a proliferation of mobile devices such as Smartphones and laptops, enables people to work almost anywhere they choose.

Along with the changing work environment, there's been a corresponding change in today's business model. Companies now depend as much on vendors, partners, and global suppliers outside organizational boundaries to get their work done as they depend on their own employees.

While this dynamic new world of work offers many benefits to individual workers, it also creates new challenges for IT administrators. For instance, IT administrators must enable employees to share data and work collaboratively with colleagues, partners, and customers on and off the corporate network but simultaneously ensure the security and integrity of the organization's digital assets.

Many organizations circumvent security measures entirely, for example, by allowing employees to share data through email. Other organizations take genuine but haphazard approaches to solving the problem of data accessibility. Some network administrators open ports in the firewall to allow access by certain protocols. Others institute virtual private networks (VPNs) that allow known remote workers to tunnel into specific systems inside the firewall. And some build extranets in the perimeter zone (also known as the demilitarized zone) outside the main firewall of the organization. Each of these options, however, requires significant implementation and maintenance time for IT administrators. And each is still vulnerable to failures and focused attacks. The Microsoft Office Groove

[1] Results presented by ITAC from the Dieringer Research Group's 2004 -2005 American Interactive Consumer Study, October 4, 2005. http://www.workingfromanywhere.org/news/pr100405.htm

2007 platform provides IT administrators with a better option for supporting cross-organizational collaboration while maintaining rigorous security standards.

The Office Groove 2007 Platform

Office Groove 2007 enables information workers to collaborate effectively across organizational boundaries while ensuring that IT administrators maintain centralized control. Organizations using Groove 2007 benefit from its ability to facilitate the sharing of information quickly and securely among those who need it.

The Office Groove 2007 platform consists of two primary components: the Office Groove 2007 client software that installs directly on each user's PC, and the server software that extends Groove 2007 client software with centralized management, data relay, and data integration services. While all enterprise customers deploy Groove 2007 for their client software, they have two choices for server software based on the size of deployment and required functionality: Microsoft Office Groove Server 2007, which is installed and maintained by the customer, or Microsoft Office Groove Enterprise Services, which is hosted and maintained entirely by Microsoft.

Office Groove 2007

Office Groove 2007 is a rich, Microsoft Windows®-based client software application that enables small teams to work together dynamically right from their computers.

The rich client and decentralized premise of Groove 2007 is what sets it apart from other collaborative workspace software solutions. All application logic and data in this Win32 application is stored locally on the desktop of each member of a workspace, providing users with full access to content and functionality whether they are online or offline. Users create workspaces right on their computers without worrying about server space or IT assistance. They invite team members to workspaces with a few clicks, creating a trusted, private group within or across the organization. Groove 2007 employs its own PKI to help ensure data remains protected on users' desktops as it crosses wireless or wired networks.

When in a workspace, a team can work together in context in real time and over time, whether they're together in the same conference room or in different organizations around the world. Every change made by each member of the workspace is automatically encrypted, transmitted to the desktops of other members, and synchronized.

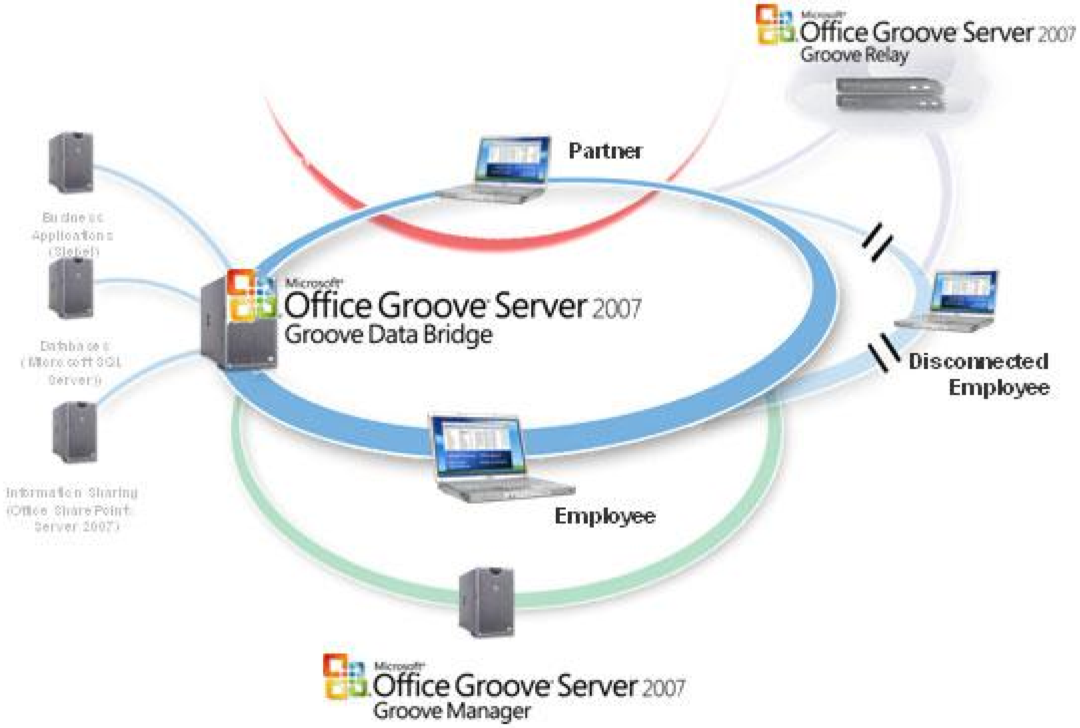
Office Groove Server 2007

While Groove 2007 enables teams of information workers to collaborate directly in a secure, decentralized manner, Office Groove Server 2007 provides the server software and tools that IT organizations require to deploy, manage, and integrate Groove 2007 across the enterprise.

Office Groove Server 2007 is a set of three separately installed server software applications that run on Microsoft Windows Server® 2003:

- **Office Groove Server 2007 Manager** provides management services such as account configuration, policy setting, and usage reporting. The Groove Manager has an optional installation configuration of Audit Server.
- **Office Groove Server 2007 Relay** provides data relay services to transmit data between Groove 2007 clients when they cannot connect directly.
- **Office Groove Server 2007 Data Bridge** provides a centralized platform for integration services to enable developers to build custom solutions that connect Groove 2007 workspaces with centralized enterprise data sources.

Figure 1: Office Groove 2007 Deployed with Office Groove Server 2007


Microsoft Office Groove Server 2007
Groove Relay
Partner
Business Applications (Siebel)
Databases (Microsoft SQL Server)
Information Sharing (Office SharePoint Server 2007)
Microsoft Office Groove Server 2007
Groove Data Bridge
Disconnected Employee
Employee
Microsoft Office Groove Server 2007
Groove Manager

Office Groove Enterprise Services

Microsoft Office Groove Enterprise Services is designed for the small to mid-sized organization, or for larger enterprises that want to deploy Groove 2007 only to a small sub-set of users within the enterprise, such as a specific workgroup, department or office.

Microsoft Office Groove Enterprise Services is comprised of two components:

- **Groove Enterprise Services Manager**, which provides Web-based management services such as account configuration, policy setting, and usage reporting.
- **Groove Enterprise Services Relay**, which provides data relay services to transmit data between Groove 2007 clients when they cannot connect directly.

Enabling More Secure Collaboration

Groove 2007 has been designed to enable effective collaboration across organizational boundaries without compromising data security or requiring extensive intervention by IT staff. To enable more secure collaboration, Groove 2007:

- **Uses standard Web protocols to cross firewalls**. Until now, allowing users to securely collaborate with others outside of their organization meant enlisting IT resources to set up a virtual private network (VPN) or alternative solution, such as a secured, shared Web site. With Groove 2007, users are empowered to collaborate through firewalls securely, with no extra effort required by IT. Groove 2007 firewall transparency uses standard Web protocols to avoid requiring network administrators to open special ports in the firewall.
- **Encrypts all content on disk and over the network**. Groove 2007 automatically encrypts all user accounts, workspaces, and their contents locally using 192-bit encryption. Furthermore, all content and activity within a workspace that is sent across the network is also encrypted and can only be decrypted by other members of the workspace.
- **Provides user–driven workspace access control**. Role–based access control is a security feature that most organizations want, but, in practice, find unwieldy to implement. Traditionally, IT resources are required to move users into separate access control lists. After initial setup, these access control lists remain static and inflexible. Groove 2007 pushes the power to determine user permissions to the manager of each workspace. With Groove 2007, setting the role of a workspace member and configuring access rights take just seconds.
- **Ensures the highest security by default**. The key to effective security for an organization is widespread adoption and usage. Groove 2007 ensures compliance by making its many security mechanisms transparent to end-users. Most aspects of Groove 2007 security are “always on,” and do not allow users to “opt out” of their use.

Underlying these capabilities is the use of public key technology for strong member authentication, data privacy, and data integrity using standard cryptographic algorithms[2].

The Groove 2007 environment also ensures the availability and integrity of enterprise data. The Groove 2007 decentralized architecture and synchronization protocols distribute data among member devices so that, in the event of catastrophic device failure such as a disk failure, data can be restored from other devices maintained within the workspace. The security framework required to meet the criteria for information assurance and the rationale behind the National Information Assurance Partnership (NIAP) evaluation effort assures the privacy, integrity, and authenticity of restored data.

Perhaps the best feature of Groove 2007 security, from the users' viewpoint, is that users hardly notice it. The only security features that standard Groove 2007 users need to manage are a password. PKI-enabled UI indicators and digital fingerprints[3] can be used to verify digital identities. All other Groove 2007 security features are transparent to the user.

The remainder of this paper explains the Groove 2007 security model in detail, with a focus on its key strengths and integration within existing security infrastructures. User responsibilities, a necessary part of any security strategy, are also covered.

[2] The core set of Office Groove 2007 algorithms and security functions are currently undergoing Federal Information Processing Standard (FIPS) 140-2 compliance as validated by the National Institute of Standards and Technology (NIST) through its Cryptographic Module Validation Program (CMVP). The standard (FIPS Publication 140-2) specifies security requirements for modules that perform cryptographic operations.

[3] A Digital Fingerprint is a human-readable representation of a user's unique and un-forgeable security credentials. Fingerprints are described later in this paper.

The Office Groove 2007 Security Model

Groove 2007 provides a collaborative environment where teams can share documents, exchange instant messages, hold threaded discussions, monitor the online status of other team members, and more. Teams using Groove 2007 work together in collaborative workspaces that place all team members, communications, tools, and information in one convenient location accessible on each member's computer. Groove 2007 users can create new workspaces and invite other users within and outside of the corporate network to join as members. It requires no special permissions on the network or any extensive IT support.

Joining a workspace provides a user with access to all the tools and content in that workspace. To join a workspace, a user simply accepts an invitation from another workspace member. Groove users can join multiple workspaces, and they can access those workspaces on multiple devices—a workstation at the office, a desktop computer at home, and a laptop for mobile use, for example. A user may also have multiple Groove 2007 identities. Workspaces are dynamic: users join and leave; data grows and shrinks; tools come and go; the lifetime of a workspace may be a few days or it may continue forever.

Within this dynamic environment of complex, changing relationships, Groove 2007 maintains proper user-to-data associations across multiple devices. Behind the scenes, Groove 2007 quietly provides authentication, data privacy, and data integrity to bind Groove 2007 identities to the people using them and to ensure the confidentiality and integrity of data as it propagates through the system. Groove 2007 access control adds an additional layer of information assurance, regulating what members can do with protected objects contained in the workspace.

Authentication

The Office Groove 2007 security model is firmly based on an authentication mechanism that binds a user's identity to specific actions within a Groove 2007 environment.

Authentication serves two purposes in that it associates:

- Electronic identities within the system with the human users they represent.
- An action within Groove 2007 (such as a modification to a file, a chat message, or a keystroke) with its electronic identity.

Binding Users to their Electronic Identities

The initial association of a user with his or her computer identity begins when Groove 2007 is first configured on a device. The first configuration step is the creation of an account (an encrypted XML object store), which includes attributes defining that user. Some account attributes are listed here in schematic XML form. The indentation indicates a hierarchy wherein an account may contain multiple identities, such as a personal identity and a professional identity. Each identity has its own unique parameters, including sets of keys and contact information.

```
account
        {identities}
                identity_1
                        {spaces}
                        private signing key (for Identity 1)
                        private encryption key (for Identity 1)
                        contact information (for Identity 1)
                        id-url
                        public key algorithms
                        public signing key
                        public encryption key
                        devices
                        relay server
                identity_2
```

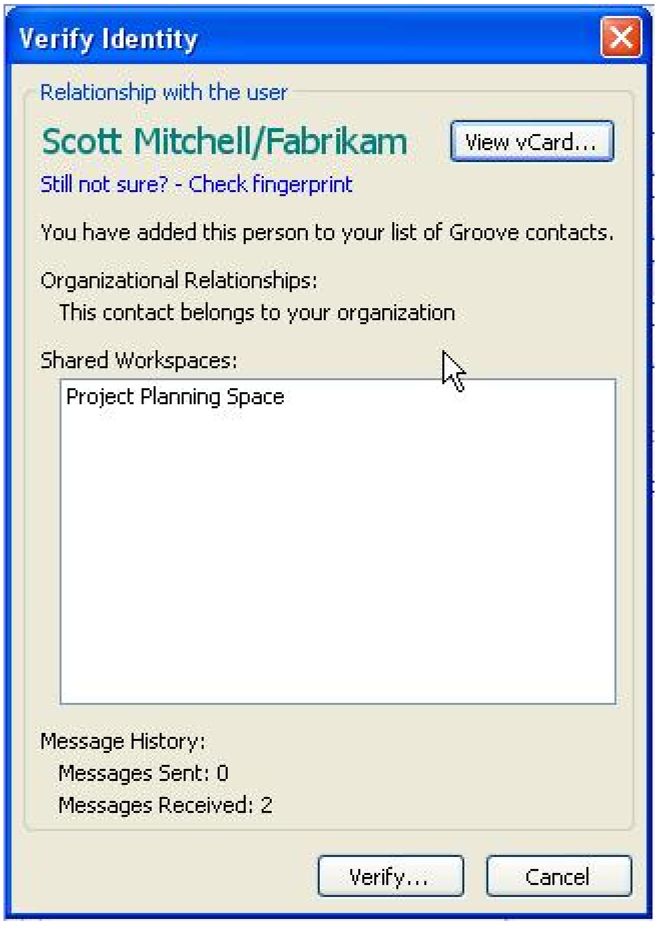
Once a user creates an electronic identity, for example, Alice, other users need a way to verify that an electronic identity truly belongs to Alice. In a managed environment, members of a Groove domain are automatically authenticated with other members of that domain. In an unmanaged environment, it is up to the individual to establish the appropriate level of authentication. Likewise, with e-mail, it is up to the recipient to verify that a message actually originated with the person who is identified as the sender—and few people bother to take that additional verification step. By providing a built-in authentication mechanism, Groove 2007 helps users protect themselves from spoofing and man-in-the-middle (MITM) attacks.

Groove 2007 offers several ways for users to authenticate the electronic identities of other members of workspaces.

- **Direct peer-to-peer authentication via digital fingerprints.**
  Groove 2007 supports authentication of users through a centralized PKI certificate authority or by manual authentication. In the manual scenario, users examine the digital fingerprints of other users' public keys. Digital fingerprints are hexadecimal strings generated dynamically using a secure hash algorithm (SHA-1, approved by Federal Information Processing Standards) to hash a user's public keys. Fingerprints are easier for people to read than public keys, yet just as secure. Public keys, which Groove 2007 uses to verify signatures on messages, travel in a user's *contact information.* The contact information is a user's electronic identity; it can be stored in the Groove Public Directory on local directory servers where it's readily available to other users.

  Fingerprint-based authentication involves contacting the person using an out-of-band means such as a phone call to confirm their fingerprint value is correct. The Verify Identity dialog (see Figure 2) indicates that Scott Mitchell is a known contact based on common membership in the "Project Planning Space".

Figure 2: Authenticating a user



Verify Identity

Relationship with the user

Scott Mitchell/Fabrikam

Still not sure? - Check fingerprint

You have added this person to your list of Groove contacts.

Organizational Relationships:
This contact belongs to your organization

Shared Workspaces:
Project Planning Space

Message History:
Messages Sent: 0
Messages Received: 2

- **Office Groove 2007 (application-specific) PKI authentication**
  In a managed environment, Groove 2007 supports automatic authentication, relying on certificates (signed contact information) issued by certification authorities (CAs) in Groove Manager. Each Groove Manager domain acts as a certification authority and certifies contact information for all users in its domain. For managed users, Groove 2007 automatically validates certificates of other users within the management domain using the domain's CA certificate. Additionally, domain administrators can create cross-domain certificates (containing the public key of a foreign domain), allowing users to (automatically) authenticate users in other domains.

- **Enterprise PKI Integration (in lieu of Groove 2007 PKI) authentication**
  An organization that already deploys a general-purpose enterprise PKI can enable use of their corporate PKI in lieu of Groove 2007 PKI for authenticating contacts. In this mode, users' Enterprise PKI identities are propagated into Groove 2007 by linking their Enterprise credentials to their Groove 2007 contacts. When presented with an enterprise-PKI-enabled contact, Groove 2007 automatically validates the containing certificate with the corporation's enterprise PKI. In essence, Groove 2007 behaves simply as a PKI-enabled application, leveraging Microsoft's standard CryptoAPI architecture. This option is only available to organizations that deploy Office Groove Server 2007 onsite.

Groove 2007 users (and their administrators) have a powerful and flexible toolbox for authentication by mixing and matching the three authentication mechanisms Groove provides. The Groove 2007 user interface highlights contact authentication states by presenting the information in a non-intrusive yet obvious manner. Where names of contacts are listed, they are color-coded according to their authentication states as follows:

- **Black**: The contact is neither authenticated nor certified.
- **Green**: The user has directly authenticated the contact.
- **Teal**: The contact is certified and is a member of the user's organization (currently supported with Groove 2007-PKI only).
- **Blue**: The contact is certified (either through Groove 2007-PKI or Enterprise-PKI).
- **Red**: The contact's name conflicts with that of another contact. The user is advised to resolve this conflict; otherwise, it can lead to name-spoofing attacks.

In summary, the initial binding of a human user to his or her signing keys forms the basis of trusted authentication within the Groove 2007 system. A fingerprint or certificate confirms the link between a human user and his or her electronic identity. Organizations can decide for themselves which authentication method(s) to adopt based on their user requirements and security standards.

Linking Actions to Electronic Identities

The second requirement of authentication is to accurately map actions in Groove 2007 workspaces to electronic identities. Using public key signature technology, Groove 2007 manages “data authentication” behind the scenes for all communication between Groove 2007 users. Groove instant messages are signed with 2048-bit RSA keys, while incremental changes to workspace data are signed with 1536-bit ESIGN keys (for their performance advantage over RSA keys). Users do not notice the data authentication service. It is provided automatically and silently. To learn how a receiver obtains a sender’s public key for authenticating messages, see Office Groove 2007 Workspace Security in Action. For information about how public key technology is used for signing data, see Security Technology Definitions in Appendix A.

Data Privacy and Integrity On-Disk

Users can log in to their Groove 2007 account with either a password or a smart card. With either method, the user’s Groove 2007 account is protected (encrypted and integrity protected) on-disk with a variety of cryptographic keys. An additional administrative data access key is used in managed environments to gain access to a user’s account by an administrator.

Password Login

A Groove password can contain upper and lower case letters, punctuation (including spaces), and numerals. IT administrators can set policies regulating password strength (specifying composition and expiration) through Groove Server Manager or Groove Enterprise Services Manager. Following industry best practice, passwords are not stored on disk. Groove 2007 processes users’ passwords with a cryptographic algorithm called PBKDF2 (Password-Based Key Derivation Function #2, see RFC 2828). PBKDF2 derives cryptographic keys from two auxiliary parameters called *salt* and *iteration count*. These parameters help thwart guessing attacks.

The salt protects passwords against dictionary attacks, so an attacker cannot pre-compute a single "hacker's dictionary" for use against all Groove 2007 users. Groove has always used a strong 20-byte random salt.

Iteration counts determine the length of time it takes to map passwords to keys: the slower the mapping, the fewer guesses an attacker can make per unit of time. Office Groove 2007 uses "smart iteration counts." That is, it computes at run-time (and verifies at each log in) the iteration count value that results in a mapping time of about a quarter-second. This represents a significant increase in password security with no inconvenience to users.

Groove also provides the option for users to have their system "memorize" their password. When this option is selected, Groove protects the memorized password using DPAPI.

Smart Card Login

Alternatively, users can log in to their accounts with a smart card, if smart cards are supported by policy in managed environments. Groove 2007 software automatically detects registered smart cards on the device and allows them to be used. The smart card log in feature affords extra protection since account entry requires "something you have" instead of merely "something you know" (that others can possibly guess). Groove 2007 software leverages whatever smart card authentication mechanism an organization chooses to use: a PIN and/or a biometric mechanism such as a fingerprint or retinal scan.

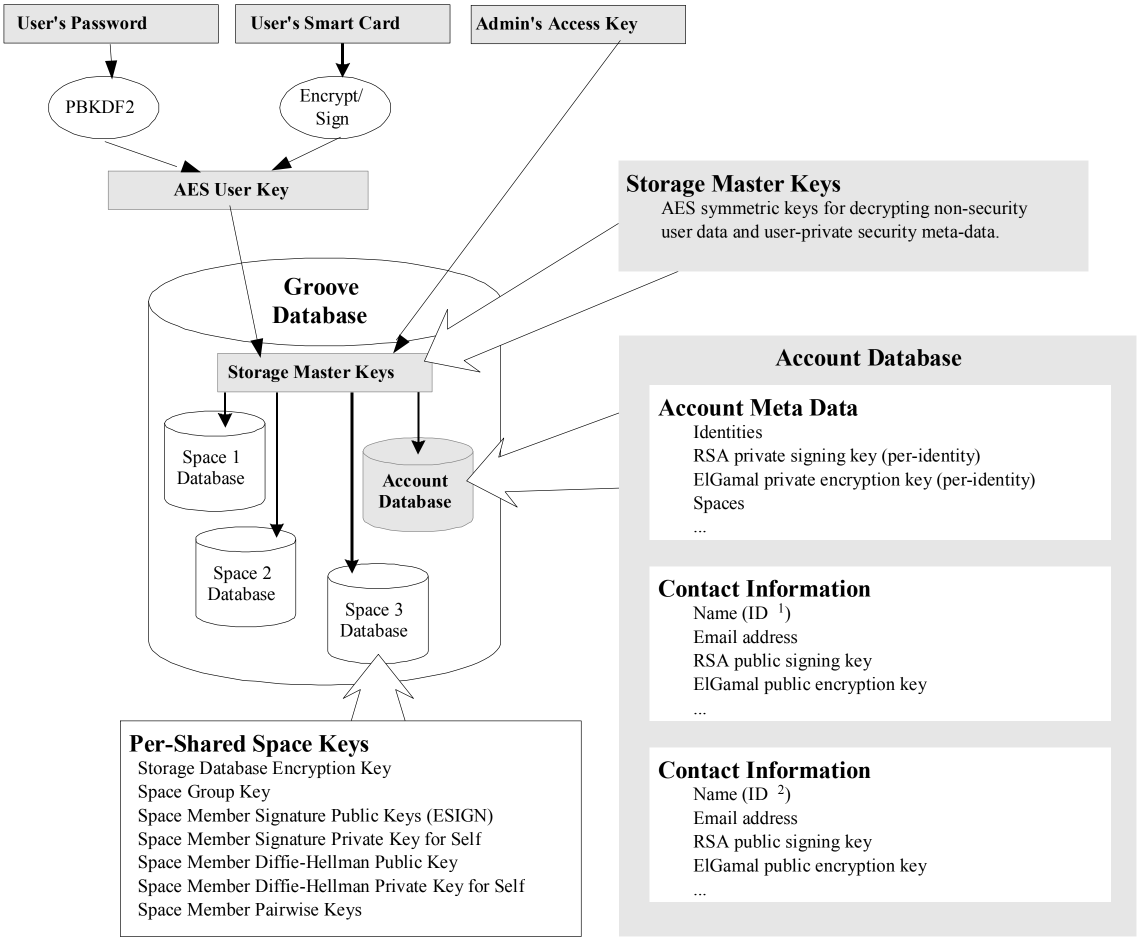
Administrative Data Access

In managed environments, administrators can gain access to a user's account using an administrative data access keypair. This keypair is automatically generated on Groove Manager with optional policies to distribute its public key to all or a subset of the users' accounts. The data access public key is then used to encrypt the user's Storage Master Keys, allowing the administrator's data access private key to be an entry point into the user's account. For information on two different access modes supported, see "Master Keys" section below.

User Account and User Data Cryptographic Keys

The user key is either (a) derived from the user's password or (b) randomly generated and protected with the user's smart card credentials. Access to the Storage Master Keys (either through the user key or the administrator's key) provides ultimate access to the user's account and workspaces. In figure 3, gray shaded boxes are components directly derived from or decrypted when users log into their Groove 2007 accounts. For efficiency, workspaces and their data remain encrypted until the user explicitly opens them. When a user opens a file from a Groove workspace, Groove 2007 uses Windows Encrypted File System (EFS) to encrypt the temporary files. (Also for efficiency, individual data within databases are decrypted and accessed only when needed.)

Figure 3. Groove 2007 Key Hierarchy


User's Password
User's Smart Card
Admin's Access Key
PBKDF2
Encrypt/ Sign
AES User Key
Storage Master Keys
AES symmetric keys for decrypting non-security user data and user-private security meta-data.
Groove Database
Storage Master Keys
Space 1 Database
Space 2 Database
Space 3 Database
Account Database
Account Database
Account Meta Data
Identities
RSA private signing key (per-identity)
ElGamal private encryption key (per-identity)
Spaces
...
Contact Information
Name (ID 1)
Email address
RSA public signing key
ElGamal public encryption key
...
Contact Information
Name (ID 2)
Email address
RSA public signing key
ElGamal public encryption key
...
Per-Shared Space Keys
Storage Database Encryption Key
Space Group Key
Space Member Signature Public Keys (ESIGN)
Space Member Signature Private Key for Self
Space Member Diffie-Hellman Public Key
Space Member Diffie-Hellman Private Key for Self
Space Member Pairwise Keys

Following is a detailed description of some of the keys Groove employs to protect user accounts and data:

- **AES User Key**. This key is used to encrypt Storage Master Keys.

  In the case of password login, this is a 256-bit AES[4] symmetric key derived from the password using PBKDF2. It exists only temporarily in memory, is zeroed after use, and is never sent over the wire. The same password used on another device will generate a different symmetric key due to the random salt value that is passed to PBKDF2.

  In the case of smart card login, this is a randomly generated 192-bit AES key encrypted with the smart card's encryption public key, and signed with the smart card's signature private key. At login, the smart card's decryption private key decrypts this key, and the smart card's signature public key verifies the signature on this.

- **Master Keys.** Master keys are keys that protect other keys.

  There are two main master keys associated with Groove 2007; both are 256-bit AES symmetric keys. The security metadata master key protects keys that encrypt user security metadata (user's cryptographic keys), while the data-only master key protects keys that encrypt non-cryptographic user data (for example, tool and contact data).

Why two kinds of master keys? In managed environments, Groove 2007 supports two kinds of administrator access mechanisms (controlled by policy settings): (1) user data access (with no access to user crypto secrets) and (2) user login credential reset (with full access). The former gives the administrator access to the user's data, including workspaces and instant messages, without the ability to masquerade as the user. In this mode, the administrator's public key encrypts only the data-only master key. The latter mechanism is more powerful and risky, giving administrators full access to the user's entire data set. In this mode, the administrator's public key encrypts both the security metadata and data-only master keys.

[4] Advanced Encryption Standard specified in FIPS Publication 197. The Office Groove AES implementation is presently being evaluated for FIPS 140-2, level 1compliance.

Account database
When a user logs into Groove 2007, information identifying the user's workspaces and messages is generated from data contained in the account database. The account database also contains certain user-private metadata about the account itself:

- Private keys associated with the identities held by the account (an account can hold multiple identities). Each identity is associated with two key pairs (called "identity key pairs"):
    - A 2048-bit, asymmetric RSA key pair used for signing messages (instant messages and workspace invitations/acceptances) outside the context of a workspace. This key pair also signs the per-workspace signing keys that use the ESIGN algorithm.
    - A 2048-bit, asymmetric ElGamal key pair used for encryption of messages outside of the context of a workspace.
- Personal contact information for each identity. Each contact includes individual and professional identity name, phone number, e-mail address, and so on. Contacts also contain some public information, such as the public halves of the RSA and ElGamal keys used for verifying and encrypting messages between identities outside the context of a workspace.

Workspace encryption key
When a user creates a workspace, Groove 2007 adds information about the workspace to the account database and then generates a storage database encryption key: a device-local 192-bit per-workspace symmetric key that encrypts stored workspace data. This key also derives a 192-bit per-workspace symmetric key that integrity-protects stored workspace data. Workspace members locally generate their own values for this key.

Data Privacy and Integrity "Over the Wire"

Information held in Groove workspaces is encrypted on a user's computer and any changes made to the data are encrypted when they are shared with other workspace members "over the wire." As the data travels to the other workspaces and when it arrives, it is also encrypted on all the other members' PC's as well. Even when data is waiting to be delivered to an offline user, it's encrypted. It isn't decrypted until the authorized user has taken it off the server and onto their local device.

During transmission, Groove uses a number of workspace keys, including:

- Workspace group key: a shared 192-bit symmetric key that dynamically derives the workspace group encryption key and the workspace group MAC (Media Access Control) key for integrity of workspace data transmitted online. The workspace group key is distributed to new members in the invitation protocol described later in this paper. The workspace group key is re-keyed (changed) when a member is uninvited from the workspace.
- Workspace member signature private key: a 1536-bit asymmetric ESIGN[5] key used by this member in this workspace to sign deltas, messages sent within the context of a workspace. The public half of this key pair is sent in the *add member* delta protocol described later in this paper. Public keys of all members are maintained here as well.
- Workspace member Diffie-Hellman[6] private key: a 2048-bit asymmetric key used by this member in this workspace for pair-wise key establishment between each pair of members in a workspace. The public half of this key pair is signed by the user's identity signature private key and distributed to the entire group in the *invitation* protocol. Public Diffie-Hellman keys of all members are maintained here as well.
- Workspace member pair-wise key: With each member of the workspace, each user shares a distinct 192-bit symmetric key for deriving two other temporary pair-wise keys. The derived keys are used to encrypt (192-bit AES) and integrity protect (192-bit HMAC SHA-1) messages (such as delta fetch requests) targeted to single users in the workspace. The workspace member pair-wise key derives from Diffie-Hellman key agreement between each pair of members in the workspace (using the workspace member Diffie-Hellman key).

Synchronizing New Member Workspace Security

Existing group members learn about new members through an *add member* delta. Add member deltas maintain the security of a workspace, managing key distribution whenever someone joins a group.

Add member delta messages, encrypted under the workspace group encryption key, include:

- **ESIGN public key:** The new member's key is included. This per-workspace key is used for message data authentication and integrity protection, binding data changes to a specific ESIGN public key within a workspace. This key is signed by its owner's identity signing key to convey its authenticity.
- **Diffie-Hellman public key**: The new member's key is included. Each recipient uses these public keys together with their own Diffie-Hellman private key to derive symmetric pair-wise keys (one for AES encryption/decryption and another one for integrity protection using HMAC-SHA-1) for protecting messages targeted to individual members of the workspace. This key is signed by its owner's identity signing key to convey its authenticity.
- **Other parameters**: Contact information, workspace and device URLs are included. Some of these elements are used not only as locators, but also as mix-in constants ("diversifiers") to derive various keys needed in a workspace.

Data Privacy and Integrity in the Groove Workspace

For general-purpose usage, Groove 2007 employs a simple hierarchy of roles and role-based permissions to enable some users to perform specific functions while limiting the actions of other users in a workspace. Groove 2007 provides the following roles:

- Manager
- Participant
- Guest

Each role maps to specific default permissions with respect to:

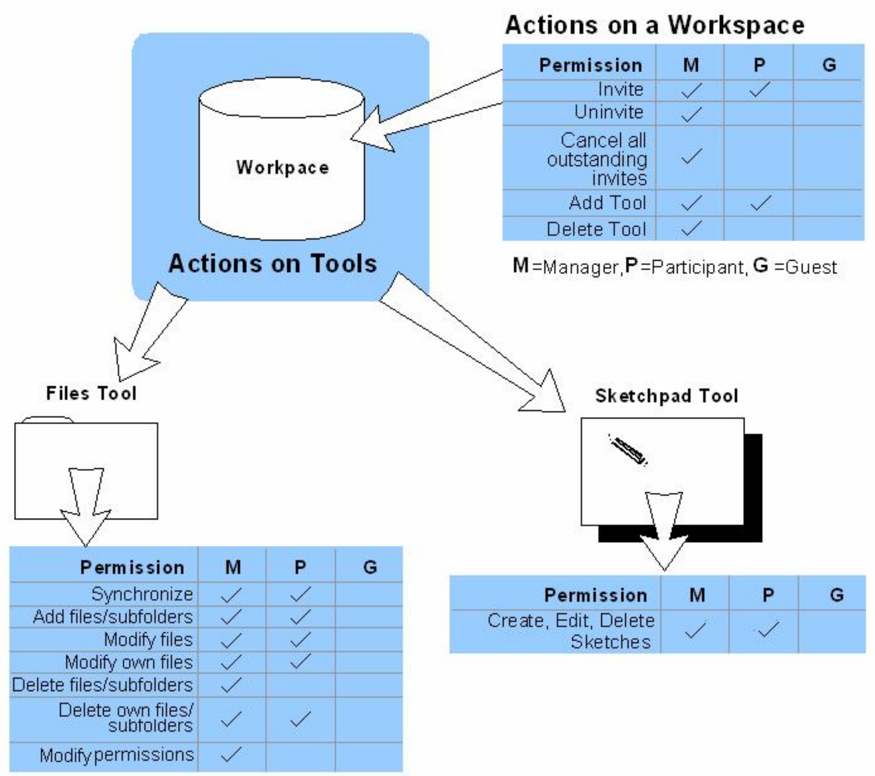
- Per-workspace actions

- Per-tool actions within a workspace

Figure 4 illustrates basic principles of the Groove 2007 role-based access control framework. The creator of a workspace is automatically assigned the role of manager. Other user-to-role mappings are assigned when users are invited to a workspace. Managers can reassign roles at any time. Users may have different roles in different workspaces. Tools have their own tool-relevant permissions.

The Groove 2007 access control facility is orthogonal to, yet dependent upon, the low-level security model primitives of authentication, confidentiality and integrity covered in previous sections of this paper. It is this added dimension that gives users direct high-level control over their environments. This is especially important in ad-hoc autonomous workspaces that have little to no centralized management.

Figure 4: Roles Regulate Actions on Workspaces



Actions on a Workspace

Permission	M	P	G
Invite	✓	✓	
Uninvite	✓		
Cancel all outstanding invites	✓		
Add Tool	✓	✓	
Delete Tool	✓		

M=Manager,P=Participant, G =Guest

Permission	M	P	G
Synchronize	✓	✓	
Add files/subfolders	✓	✓	
Modify files	✓	✓	
Modify own files	✓	✓	
Delete files/subfolders	✓		
Delete own files/ subfolders	✓	✓	
Modify permissions	✓		

Permission	M	P	G
Create, Edit, Delete Sketches	✓	✓	

Three additional security mechanisms manage how users are added and removed from a workspace:

- The Groove 2007 invitation protocol that brings new members into a workspace in a secure manner;
- The Add member deltas that inform group members about new members; and
- The Rekey deltas, which handle changing membership over time.

Inviting New Members to a Workspace

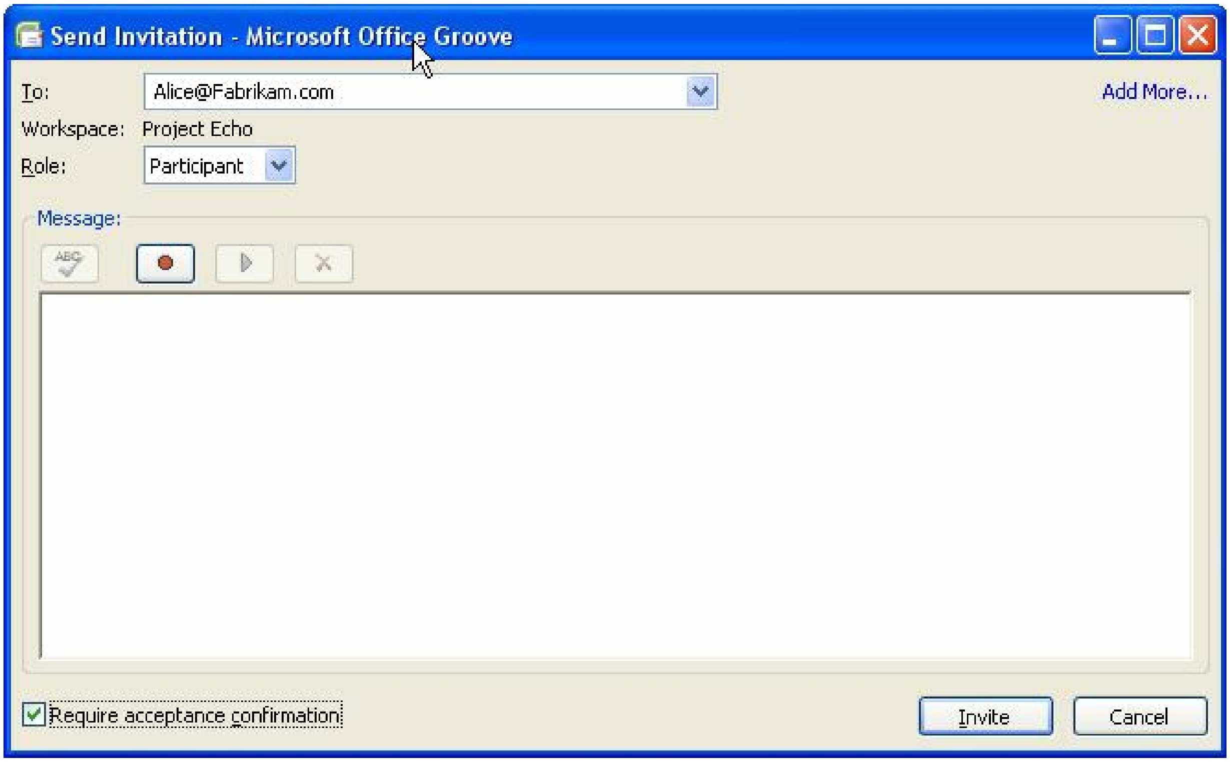
When a user creates a workspace, the user is the only member of that workspace. Any data added to the workspace is protected under keys created by Groove 2007 for that workspace. To share data, users must be invited to join the workspace. The Groove 2007 invitation protocol is the mechanism that brings new members into a workspace in a secure manner.

Following is a scenario that illustrates how the invitation protocol works. It demonstrates how a new member joins an existing workspace and how the *add member* delta informs all the other workspace participants about the new member.

Scenario: Bob uses e-mail to send an invitation to Alice who does not have Groove 2007 software installed on her machine.

Bob has created a Groove 2007 account and has created a workspace called "Project Echo." The group has only a few members: Bob, John, and Mary. Now Bob invites Alice to join the workspace. Bob opens the Project Echo workspace and enters Alice's e-mail address (as Alice is not yet a Groove 2007 user and, therefore, has no Groove 2007 contact information).

Figure 5: Inviting a New Group Member



Send Invitation - Microsoft Office Groove

To: Alice@Fabrikam.com

Workspace: Project Echo

Role: Participant

Message:

☑ Require acceptance confirmation

Note: **Require acceptance confirmation** is automatically enabled for e-mail invitations.

When all required data is entered, Bob clicks **Invite**, sending the invitation. This and all other Groove 2007 invitations contain several important elements:

- A URL for Alice to download Groove 2007 and instructions for installing it.
- The role the invitee will have (for access control purposes) in the workspace upon accepting the invitation. The default role is "participant."
- Cryptographic protocol settings used for the workspace, including Diffie-Hellman key parameters that members use to create their own pair-wise keys for private exchanges with each other.
- Bob's contact information containing his RSA and ElGamal public keys. These verify and encrypt instant messages exchanged with Bob.

Alice receives the invitation in her e-mail and clicks the link to download and install Groove 2007. Alice now has a Groove 2007 identity and her own RSA and ElGamal signing and encryption keys so she can exchange instant messages with other Groove 2007 users. She then clicks the invitation link for Project Echo in her e-mail program and accepts the invitation. If Alice is in a managed environment, she authenticates Bob automatically using her organization's Enterprise PKI or Groove's built-in PKI. Alternatively, Alice may take additional steps to authenticate Bob manually using digital fingerprints. When she clicks **Accept**, Groove sends Alice's acceptance message, which contains Alice's contact information, to Bob. Since Bob checked **Require Acceptance Confirmation**, he has the opportunity to confirm and authenticate each member before the workspace is sent.

Bob clicks **Confirm**, which sends the workspace and the shared secret key used by members of this workspace to Alice. This information is encrypted under a one–time messaging key (an AES 192-bit symmetric key). The one–time key is sent to Alice encrypted under her ElGamal public key.

Thus, the Groove 2007 security model has enabled Bob to contact and authenticate Alice, who was outside the system, and to provide her with access to the workspace with no risk that an unauthorized person could view the content of the workspace.

Before sending the workspace to Alice, another Groove 2007 security facility, called an *add member* delta, distributes Alice's keys to other members of the workspace so they learn about Alice.

Uninviting People from a Workspace

Groove 2007 includes functionality for uninviting people from a workspace. By default, only workspace managers can uninvite a member of the workspace. Uninviting someone is a passive operation from the standpoint of the person who is uninvited. A rekey delta containing a new workspace group key is sent out to each remaining member of the workspace encrypted under that workspace member's pair-wise key. The uninvited member is omitted from the rekey delta, but is sent a delta indicating he has been uninvited. This operation removes the workspace and all its data from the uninvited person's devices. The operation cannot, however, delete data the uninvitee has saved to a location outside of the workspace.

User Responsibility for Data Security

Notwithstanding the many technological and policy elements in Groove 2007 that enforce security throughout the system, people are ultimately responsible for the security of workspaces and the Groove 2007 system as a whole. Attackers of cryptographically protected systems almost always forego attacking algorithms and protocols in favor of guessing a user's password, taking advantage of a system left unattended, or subverting someone through "social engineering" attacks. Consequently, there are steps that all users can take to improve the security of their data, with or without Groove.

- Users should use strong, hard-to-guess passwords. Managed Groove environments can enforce password requirements, but users should avoid simple or obvious passwords.
- Users have the option to have their system "memorize password". When this option is selected, Groove protects the memorized password using DPAPI.
- Groove 2007 leverages local antivirus software to provide real–time scanning of files, but users, or their organizations, should take the necessary steps to ensure that virus definitions are up to date.

- Groove 2007 does not automatically log people off after a period of idle time. Therefore, users should protect their computers with password-protected screensavers.
- Groove 2007 users and Groove 2007 Server administrators should use best practices, such as installing security patches and updates as dictated by relevant security policies.

Groove Security in a Managed Environment

Up to this point, this paper has focused primarily on the security features offered by Groove 2007 client software. Security does not end at the client, however. The Office Groove 2007 system includes Groove Server 2007 software that provides centralized management, relay, and data integration services. Groove Server can be installed and maintained onsite at an enterprise or comparable services can be engaged through Microsoft Office Groove Enterprise Services (hosted by Microsoft Corporation).

The Manager and Relay applications are essential components of Groove Server, enabling centralized administration of Groove clients and helping provide efficient, secure data exchange. The security protection of these installations is discussed in more detail subsequently.

Deploying Groove 2007 in a managed environment provides additional security benefits, including a user interface that facilitates the following:

- **Centralized Policy Administration**— Provisions for centralized administration of Groove usage policy facilitate dissemination of security controls across larger environments. Domain and group-based policy options give administrators the flexibility to set policies for an entire domain, specific domain groups, or individuals. Security-related policies control account backup scheduling, password strength, identity publication, communications with users outside the domain, and other identity and device activities.
- **Account Backups**—The Account Backup file contains all the details to rebuild the user's account. Upon restore, users will have their account data, all their contacts, and a listing of all the workspaces they belong to.
- **User Monitoring**—Managed Groove clients regularly report usage statistics to Groove management servers, helping administrators secure the work environment by monitoring user activities, workspace characteristics, and Groove tool usage.

The following security features are available only to organizations that deploy Microsoft Office Groove Server 2007 on site:

- **PKI Support**—Administrators can choose between standalone Groove 2007-PKI and Enterprise-PKI integration for authentication of Groove 2007 contacts, without the need to "manually" check digital fingerprints.
- **Server Monitoring**—The Groove management server reports server events to an easily-visible audit log, helping administrators to monitor server health and track anomalies.
- **Auditing**—An optional Groove management feature provides centralized auditing of selected client events. These events are securely logged on the user’s local device, periodically and securely uploaded to a Groove Server Manager, and incorporated into a Microsoft SQL Server™ database.
- **Assignment of Relay Servers**—Administrators can assign Groove users to a sequence of Groove Relay servers, providing relay redundancy.

End-to-end security features are described subsequently.

Security Protections for Groove Server 2007

Groove Server 2007 Manager runs as an ISAPI (Internet Server API) add-in on a Microsoft Internet Information Server (IIS). Important aspects of its security include the following:

- The Groove Manager administrative interface does not have its own proprietary authentication utility, but instead relies on the Internet authentication scheme in place for controlling access to IIS.
- Enabling appropriate filters in the Microsoft IIS server platform, such as allowing administrator access only through SSL port 443 helps protect the administration interface from external attacks.
- Groove Manager provides a role-based access control system, separate from that used in Groove 2007 workspaces or in a Windows domain. This system lets you define administrators with different levels of authority to different levels of Groove management, starting with server administrator, (with top-level Groove Manager oversight), domain administrator (with domain-level oversight), member

administrator (with member-level oversight), and Report Administrator (with Groove Manager report access only)..

- Groove Manager stores data in a SQL Server database, which is installed on a separate machine. To maximize security protections, the SQL Server should be isolated behind a port-restricted and IP address-restricted firewall. It should always have the latest Critical Update Package and Security Rollup installed.

Groove Server 2007 Relay runs on separate Windows server machines, typically within a perimeter network. Important aspects of its security include the following:

- Groove Relay is intended for operation in a perimeter network or on an internal/external network boundary, with filters on the external network interfaces to allow only inbound TCP/IP traffic on ports 2492, 443, and 80.
- Port 8009 should be open for transmissions from the Groove Manager but assigned to a network interface card connected to a private internal network. Consider blocking inbound port 8009 on the Groove Relay external interface unless your Groove Manager is configured to access the Groove Relay over an external interface (on the Groove Relay server).
- Port 8010, used for browser access to Groove Relay administrative pages, is restricted to the local computer by default, prohibiting remote administrative access to achieve basic administrative security.

Security Enhancements for Groove in the Enterprise

The following sections describe provisions built into Groove Server that help promote secure collaboration among Groove users.

Identity Creation, Account Configuration, and Domain Enrollment

This section describes the protocol handshake of the various Groove 2007 components when a managed identity is created, configured, and enrolled into a management domain.

Administrators prepare their environment for Groove management by adding user information to a domain defined in Groove Manager. User information can be added manually or imported via integration with an onsite Active Directory server. In either case, the Groove Manager creates a unique account configuration code for each user and an exchange of data between Groove clients and servers results in a managed Groove identity for each user. Managed identities are members of designated Groove Manager domains through which administrators issue Groove security and usage policies and relay server assignments. This section describes the protocol handshake of the various Groove components when a managed identity is created, configured, and enrolled in a management domain.

In scenarios where users are manually added to a Groove Manager domain, the administrator sends the system-generated account configuration code and Groove Manager URL to each user via e-mail from Groove Manager. Users configure their managed accounts as instructed in the e-mail and the Groove client software contacts Groove Manager, using the account configuration code to authenticate each user.

When Groove Manager receives an account configuration code from a Groove client, it replies with a packet of identity metadata, administrator-set security policies, and relay assignments associated with the identity’s domain. With this information, the Groove client creates a managed identity which contains the cryptographic keys that help secure user data exchanges. The identity now becomes managed and is enrolled in a Groove Manager domain, where, if Groove-PKI is enabled, the identity is signed by Groove Manager, the Certification Authority. If third-party PKI is used, identities are signed by CAs defined on Groove clients.

During the process of identity creation, Groove Manager generates a random identifier and passes it as a pre-authentication token to the assigned Groove Relay server to identify the user. The user’s Groove client will present this identifier as proof of identity upon initial contact (registration) with the relay. A shared secret key establishes a mutually authenticated link for all subsequent user-to-relay data flows.

In scenarios, where user information is imported into a Groove Manager domain via synchronization with an Active Directory server, the Automatic Account Configuration feature can be used to configure managed Groove users; user action is not required. This is the recommended approach to deploying managed Groove users. In this case, Groove uses Windows credentials, instead of account configuration codes, to authenticate users to Groove Manager and an administrator disseminates the Groove Manager URL to target Groove clients via a Windows General Policy Object (GPO). Using this URL, clients contact the Groove Manager server with each user's Windows credentials, which are authenticated against user login names imported from the Active Directory server. Groove Manager responds with the appropriate identity meta-data, policies, and relay assignments, and the Groove client creates the managed identity, as described above for manual deployment.

Identity and Device Security

Groove Server 2007 Manager offers two classes of manageability within an organization, to which specific security policies can be applied:

- A managed identity within a Groove user account. In organizations where user accounts have multiple Groove identities, the Groove Server Manager can manage the corporate identity by applying policies that effect appropriate restrictions. Identity-based policies include those governing identity publication and communication with external users.
- A device (and its licensed Groove 2007 software) on which a managed user is running Groove. A device may or may not be explicitly managed. Important device-based policies include password-setting requirements and account lockout.

Centralized Policy Administration

As mentioned above, Office Groove Server 2007 Manager manages identities and devices via the distribution of policies throughout defined management domains. A security policy can be set for each management domain or group within an organization. Policies set the behavior of managed identities and devices, controlling such activities as password creation and expiration, identity publication, and creation of multiple user accounts. Policies can also restrict users from communicating with members outside their domains.

This model offers flexibility in structuring meaningful Groove policies across an organization. For example, some users may work with highly sensitive information. Such a group might be allowed to communicate with only authenticated contacts, they may be restricted to running Groove only on managed devices, and their activities may be audited. Other groups handling less sensitive data may have policies with fewer constraints.

Policies are encrypted for targeted accounts using 192-bit MARC4[7] encryption. Integrity protection and authentication of policy data uses 192-bit HMAC keys and a SHA-1 hash of the policy data.

The following are examples of two important policies:

- Groove Account Backup—Administrators can schedule regular backups of Groove accounts, an essential step toward securing data resources by protecting against loss.
- Data Access and Password Reset—An exclusive data access policy (that does not involve gaining a user password) lets administrators access user data to which they are properly authorized, but prevents malicious administrators from impersonating users Password reset policies let administrators enable users to set a forgotten password to any specified value.

These policy–setting options enable organizations to closely tailor Groove 2007 to precise security needs, optimizing the overall security of the environment.

Users Removed from a Domain

Removing a user from a management domain has security implications. Groove provides mechanisms to support this important change in status, so that when a user (managed or unmanaged) is uninvited from a workspace, the data is removed from the user’s computer and the space is re-keyed for all current members. Administrators can effect a similar change across all workspaces for a managed user either by temporarily disabling the user’s account in the domain, or by permanently deleting the account from the domain.

[7] MARC4 is the Modified Alleged RC4 algorithm. (The term “alleged” distinguishes the public-domain implementation from the proprietary version marketed by RSA Security, Inc.)

Disabling an account is a temporary status change, which an administrator can easily reverse, reinstating user accounts on their computers so that they can again access their workspaces. Deleting an account from a domain is not reversible.

When a user account is disabled or deleted from a Groove Manager domain, the following conditions result once the user receives notification from Groove Manager:

- The managed identity is disabled on devices where the identity resides.
- The managed identity is logged out of workspaces where the user is active and associated data on the user's computer is inaccessible.
- Any offline Groove devices on which the managed identity resides continue operating only until the devices return online. If data access for a particular user is desired, that must be arranged before the user is removed from the domain.
- When a managed identity is the only identity in a Groove account, the account is also disabled. No further login is possible.
- Users cannot access Groove workspaces to which their managed identities belonged.
- Files in Groove 2007 Folder Synchronization (GFS) directories are no longer synchronized, although GFS files on deleted user devices will remain intact and accessible.
- Domain identity policies are no longer in effect, but any managed devices associated with the user remain managed and governed by domain device policies.

The Role of Groove Server Relay in Groove Client Communications

Office Groove Server Relay enables uninterrupted, efficient, data transfer between Groove 2007 users. The relay service is available as a service by Microsoft (Groove Enterprise Services Relay) or as server infrastructure that organizations deploy on site in conjunction with Groove Manager (Office Groove Server Relay). Whether an organization relies on a dedicated or hosted relay server, the basic functionality is the same: this lightweight store-and-forward service facilitates data transmission between users and ensures that workspace data remains synchronized even when no two members of a workspace are online simultaneously. It is important to note that although Groove 2007 relay services play a role in Groove 2007 communications, the relay service does not have the keys necessary to decrypt those payloads. The relay service is effectively blind to all the communications that pass through it.

Office Groove Server 2007 Relay and Office Groove Services Relay offer the following capabilities:

- **Offline Support**—When a Groove 2007 user makes a change to a workspace, such as an edit to a file, the user's Groove 2007 client encrypts the data first, and then attempts to send the data packet to all other members of the workspace in a direct peer-to-peer manner. In cases where a team member is offline or can't be reached directly by the client, the sender client will automatically transfer the data to the relay service associated with that recipient, where the data is deposited in a specific queue for the recipient. When the offline recipient next connects to the Internet, the recipient's Groove 2007 client automatically retrieves that encrypted data packet from the relay queue. The recipient does not need to replicate, upload or download changes; all workspace synchronization happens transparently.
- **Firewall Transparency**—If two Groove 2007 users are separated by firewalls that will not allow inbound connections, all communication that occurs between those clients is done through relay services. Remember that the Groove client

performs the data protection services, so even though the data may be traveling across the Internet, the data is encrypted end-to-end, integrity protected and authenticated. Users can communicate across organizational boundaries even when firewalls, proxy servers, or NAT (Network Address Translation) devices prevent inbound or outbound traffic over Groove 2007 preferred Internet ports. This communication is possible as long as the client is able to initiate an outbound connection to the destination relay service. By default, Groove 2007 clients attempt to communicate through TCP/IP port 2492[8]. Administrators should open this port for outbound communications if policy permits. If this port is closed, Groove 2007 clients will attempt to communicate using port 443, or even wrap their messages in an HTTP-envelope, and use port 80 (HTTP). Relay services listen for Groove communications on ports 2492, 443 and 80. As a result, so long as the Groove client is able to initiate a connection to the relay, it is able to post and get encrypted data from the relay queues. The data is never decrypted until it has been synchronized down to the local client and its integrity has been verified.

- **Bandwidth Optimization**—Office Groove Relay Services enable users to share large files even when they are on slow connections. The Groove 2007 client assesses the size of a file, the speed of the user’s connection, and the number of members in the workspace. When it is most efficient for the user, the Groove 2007 client will send the file to the Relay Service to be "fanned out" to other members, as opposed to having the sender transfer the file to each member directly. This reduces the bandwidth required by the sender.
- **Device Presence**—Office Groove Relay Services support the Groove 2007 WAN Device Presence Protocol which enables a publish/subscribe model for the client to learn about device presence information. The Groove 2007 client uses this device presence information to determine whether to send data directly to a peer, or to send data to the queue using the Relay services.

[8] This port is registered with the Internet Assigned Numbers Authority for use by Office Groove protocols.

When a Groove 2007 account is created, it is assigned either to the relay services hosted by Microsoft or to a private relay server. The Groove 2007 client uses the public key certificate of the assigned relay to register with that relay service. Henceforth, the software always uses that specific Relay Server. User contact information includes the chosen Relay Server's URL to establish a complete communication path for other Groove 2007 users. Groove 2007 contacts learn of each other's assigned relays through the Groove 2007 v-card. When contacts exchange v-cards, either directly or as a result of joining a workspace, the contacts learn of the appropriate relay contact information.

When the user account registers with a Relay Server, the account establishes a shared secret key with the Relay Server that provides a mutually authenticated link for all Relay-to-workspace communication. The secret key, shared solely with that user account, prevents a false user or Relay Server from mounting a denial-of-service attack on the system (intercepting messages targeted for another).

The Relay Service can access only message header information needed to locate devices or a target device's Relay Server. Groove 2007 end-to-end data encryption prevents the Relay Service from reading the data inside messages.

Integrating Enterprise Data into a Workspace

The Office Groove Server 2007 Data Bridges provides a Web services-enabled data access tier that integrates Microsoft Office Groove 2007 workspaces with other applications and databases in an organization's IT infrastructure. An Office Groove Server 2007 Data Bridge installed within a company's data center provides a secure centralized access point for hosting Groove 2007 workspaces and fits naturally into services-oriented architectures. Office Groove Server Data Bridge (Office Groove Data Bridge, henceforth) gains access to Groove 2007 workspaces through an administrator-created identity that can be invited to workspaces. Once resident on a Data Bridge server, a Groove 2007 workspace inherits a rich set of platform Web services that process XML-based calls from other applications in the data center. In this way, Office Groove Data Bridge functions as a data access tier, moderating data and process integration between Groove workspaces and other applications and processes, such as Microsoft SharePoint® sites and Windows Workflow Foundation.

The Data Bridge server application shares many of the same qualities with a Groove 2007 client. It relies on an underlying Groove 2007 application, communicates with Groove 2007 peers using the same Groove 2007 peer protocols, and hosts identities that participate in workspaces.

Office Groove 2007 Web Services enable the development and deployment of integration solutions that take advantage of services-oriented architectures (SOAs). The integration logic resides outside of Office Groove Data Bridge processes. For example, an external archiving program may retrieve data from a Groove 2007 Files tool for storage in a library maintained on a SharePoint site. The Data Bridge identity processes Web services calls from the custom retrieval program and mediates data exchange between the SharePoint site and Groove workspaces of which it is a member. The custom integration program resides on the retrieval application server.

The inherent cryptographic security in Groove 2007 is intended to keep workspace data and activities within the exclusive purview of the workspace member users. However, Office Groove Data Bridge identities, like Groove 2007 users, may hold membership in multiple spaces and retain access to external applications. Therefore, exercise caution when defining the presence and role of an identity in a given workspace.

The Office Groove Data Bridge server is logically located on an organizational network to allow the smallest number of Internet protocols through. On the Data Bridge server, this typically means leaving outbound port 80 open for HTTP (inbound blocked) and leaving port 2492 open for SSTP, using firewalls to block all other Internet traffic.

In the context of SOA-based integration solutions through Office Groove 2007 Web Services, consider the following information:

- Office Groove Data Bridge uses SOAP, a standard, XML-based protocol, to communicate with remote applications which are integrated with Groove 2007 workspaces through remote Groove 2007 Web Services. Native Groove security does not protect the connections between Data Bridge servers and the remote applications where the integration logic (code) lives; these are the remote applications. Therefore, pay careful attention to the security of these network connections when planning deployment. As an extra precaution, organizations can change the default network listening ports used on the remote Office Groove Data Bridge (for XMLRPC and SOAP over HTTP communications).
- All connections to devices running external applications (those integrating with Groove 2007 workspaces through Groove 2007 Web Services on Office Groove Data Bridge) should be secured with standard techniques such as IPSec and Secure Shell (SSH). Also, as standard practice, both remote and physical access to the devices should be limited to authorized administrators only. Note that Groove 2007 Web services access must be enabled on the Office Groove Data Bridge server in order to allow Office Groove Data Bridge to receive messages from external applications that rely on XML-based calls to Web services.
- Office Groove Data Bridge expects Web services calls through HTTP and does not support HTTP authentication. Office Groove Data Bridge does not support HTTPS and its associated encryption of transmitted data. Therefore, external security measures cited are highly recommended to help secure Web services communications with the Data Bridge server.

- To help prevent DNS-based security attacks, identifying the Office Groove Data Bridge server by a static IP address (rather than its DNS address) is recommended. How an organization implements security measures depends largely on the organization’s specific security requirements, the software it uses, and its existing network topology.

For more information about securing Office Groove Data Bridge communications, see *Groove Server 2007 Data Bridge Administrator’s Guide* available at http://www.microsoft.com/technet/prodtechnol/office/grooveserver/default.mspx

Conclusion

Microsoft Office Groove 2007 is software that enables teams to work together securely over the Internet as if they were in the same location. The promise of Groove 2007 is to bring people together in a workspace where they can share ideas and work collaboratively, trusting in each other without worrying whether the underlying technology breaches that trust.

The Groove 2007 security model delivers on that promise through its end-to-end authentication, encryption and integrity protection. Many of the mechanisms used to maintain a secure Groove 2007 environment are automatic and transparent to users, so as not to disrupt their work or require extensive IT support. Groove 2007 carefully balances algorithm and key strength against performance demands and closely matches them to the job at hand.

Organizations that use Office Groove Server 2007 or Microsoft Groove Enterprise Services benefit from centralized management features that offer fine-grained tailoring of policy to specific user needs and enforce organizational security policy both inside and outside the firewall. Its standalone PKI functionality helps to automate authentication across an environment. When Office Groove Server is deployed onsite, the Groove 2007 client is a PKI-enabled application for corporations that want to leverage existing PKI environments into Groove 2007.

Finally, the Groove 2007 decentralized architecture and its secure protocols ensure the robustness and availability of data within the Groove 2007 environment. These characteristics are not optional in organizations where information assurance is a high priority.

Collectively, the security features built into the Groove 2007 platform demonstrate Microsoft's commitment to Trustworthy Computing. Microsoft strives to make all of its tools and platforms secure by design and by default. In keeping with Microsoft's defense-in-depth approach to protection, the Groove 2007 platform is designed to help ensure the trustworthy identity of all its users, to help manage policy that dictates what resources those users can access, and to help protect information for its lifetime, wherever it is stored.

Appendix A

Security Technology Definitions

This paper assumes that readers are familiar with the basic concepts of cryptographic technology such as data encryption, decryption, authentication, and integrity checking. With the exception of the brief definitions that follow, the paper does not discuss the fundamental principles behind them.[9]

- **Secret Key Encryption**—Data is encrypted and decrypted using the same symmetric key. The secret key must be securely distributed to those who need it. Secret key encryption is much faster than public key encryption (described below), and is the basis for standard encryption algorithms such as AES and DES.
- **Public Key Technology**—Data is encrypted and decrypted using two mathematically related, yet distinct asymmetric keys. One of these keys is made public (it can be known by anyone), and the other remains private, known only to the keypair's holder. Public key encryption is often used to securely send symmetric encryption keys over the network. For that usage, the public key is used to encrypt data targeted to the keypair holder, and the corresponding private key is used to decrypt it.

  Public key technology is also known for its complementary ability to sign data. In this case, the signer uses his or her private key to generate a cryptographic block of the data. This block is the user's signature. Any recipient can verify the signature by using the signer's public key. Cryptographic signatures cannot be forged. When properly used, signatures support guaranteed identification of the source of the data and messages, provided that the verifying public key is correctly matched to the authentic real-world key pair holder. This is called authentication, and it is discussed in detail in this paper.

[9] For detailed discussions, refer to texts such as Bruce Schneier's *Applied Cryptography (*B. Schneier, *Applied Cryptography,* John Wiley and Sons, Inc. 1996*).*

- **Hashing**—Data hashing produces a condensed form of the original data, which serves as a unique representation of the original data. The condensed form of data is called a secure hash or digest of the original. Hashing is a one-way function, meaning the original data cannot be derived from the hashed form of the data. Changing any of the input data, even one bit, produces a radically different output. Data hashes of the same type are of consistent length (typically, 20 bytes) regardless of the size of the input data.

  Cryptographic hash functions are collision free – that is, no two datasets will produce the same hash. Hashing is used internally within Groove 2007 for a number of purposes, including password management (the password is hashed to a secret key), integrity protection (by securely storing a hash of data along with the data), and signature-generation (by hashing the data to be signed before applying expensive public-key algorithms). Groove 2007 uses the Secure Hash Algorithm (SHA-1) specified in FIPS publication 180-1, for many hashing operations.

Additional Resources

Microsoft Office Groove 2007

http://office.microsoft.com/groove

Microsoft Office Groove Server 2007

http://office.microsoft.com/en-us/grooveserver/default.aspx

Microsoft Office Groove Enterprise Services

http://office.microsoft.com/en-us/grooveservices/default.aspx

Microsoft Office Groove Server TechCenter

http://www.microsoft.com/technet/prodtechnol/office/grooveserver/default.mspx

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, this document should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. The information represents the product at the time this document was printed and should be used for planning purposes only. Information is subject to change at any time without prior notice.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.