NASA Public Key Infrastructure

presented to

FPKI-BWG

Tice F. DeYoung
Applied IT Division
NASA Ames Research Center

Principal Center for Information Technology Security

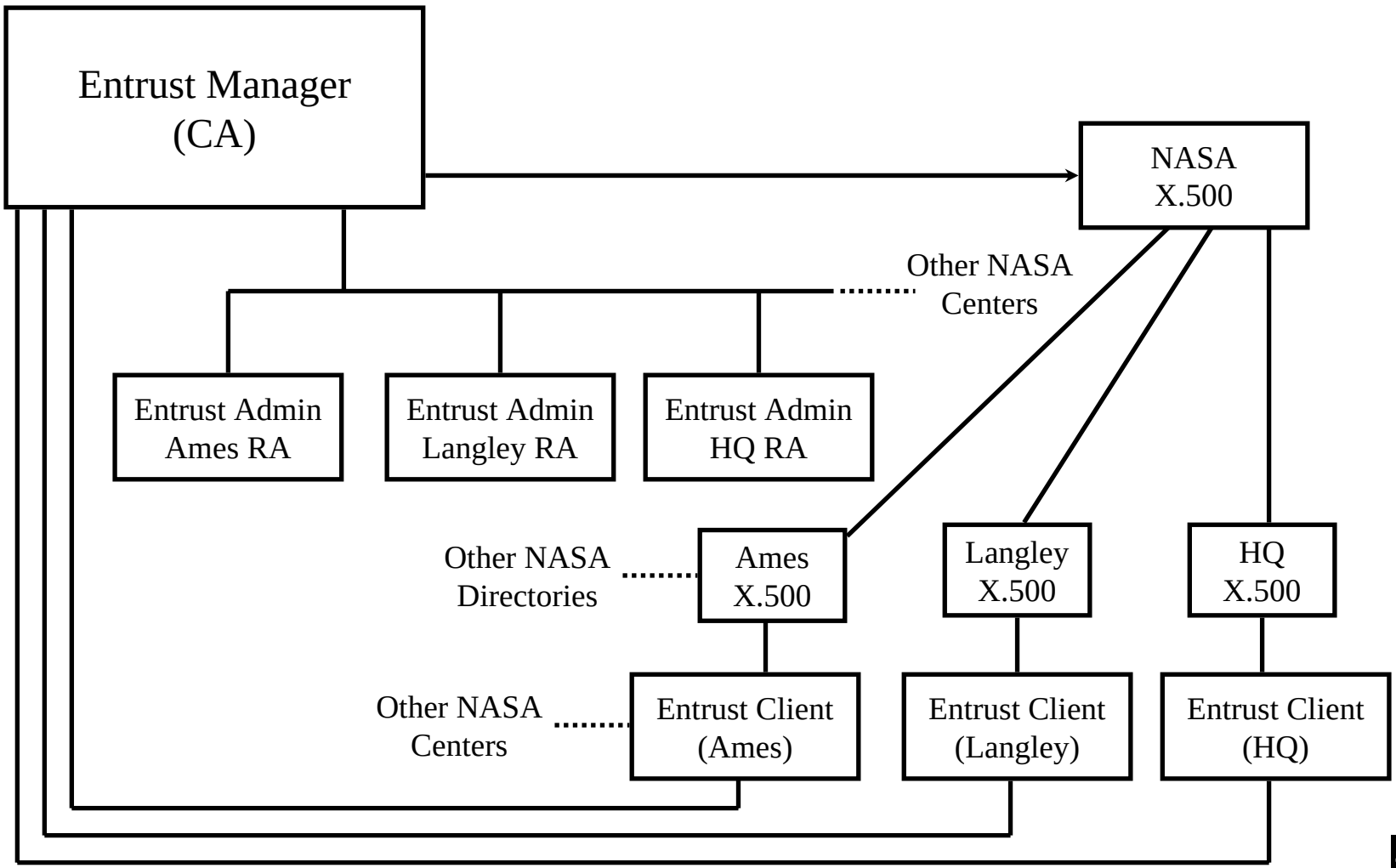
NASA PKI Components

- **Certification Authority (CA)**
  - Uses Entrust, currently version 5.0.2
  - Principal CA located and managed at Ames Research Center
  - "Hot Spare" CA at different geographic location
- **Registration Authorities (RA)**
  - RAs located at each of the eleven major NASA Centers
- **Certificate Repository**
  - Certificates are stored in the NASA X.500 Directories, which use Syntegra Mail*Hub 2000
- **PKI Policy: NASA's Policies are Defined in:**
  - X.509 Certificate Policy for NASA PKI
  - NASA Certification Practices Statement

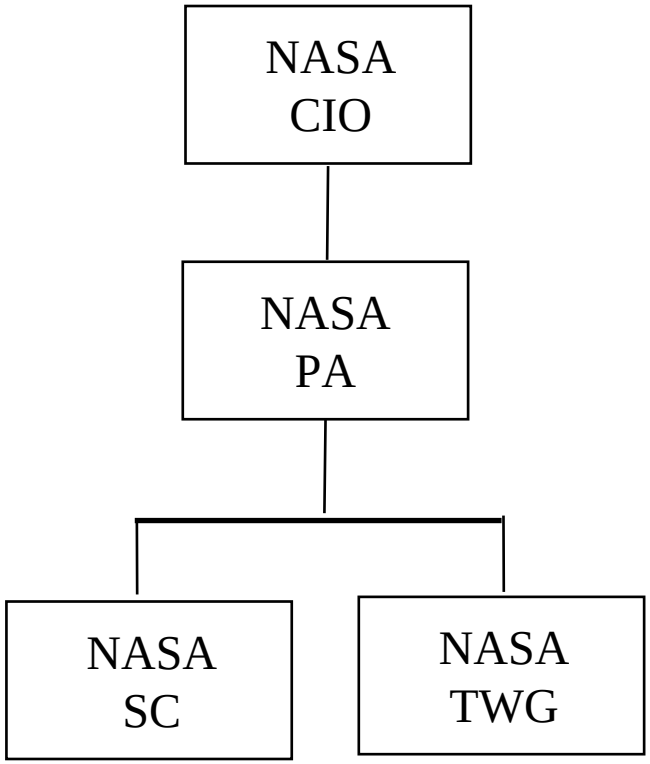
NASA PKI Software

- **Entrust Client/Entelligence**
  - Provides user certificate management and file security through encryption and digital signature
- **Entrust ICE**
  - Provides automated file security. Automatically encrypts and digitally signes files
- **Entrust Express**
  - Adds secure email capability to Microsoft's Outlook and Qualcomm's Eudora
- Entrust Direct
  - Provides web client-to-web server authentication & security

NASA PKI Diagram



NASA PKI Management



NASA PKI Management, cont.

- The NASA PA is responsible for the CP and CPS and for all PKI policy decisions
- The NASA SC is responsible for establishing NASA Enterprise requirements for PKI
- The NASA TWG is responsible for coordinating PKI rollout and for PKI application development

NASA PKI Status

- Operational Since 2000
- All Eleven Centers Passed Operational Readiness Reviews Prior to PKI Rollout
- Approximately 3,000 Certificates Issued to NASA Personnel & On-Site Contractors
- Operating at Medium Level of Assurance Only
- Agency Functional Offices Are Adopting PKI for Secure Messaging: Agency Has a Metric for This
- Mission Areas Are Investigating Use of PKI

NASA PKI Recent Accomplishments

- Applied for & Received Funds for Cross-Certifying with FBCA
- Enhanced NASA X.500 Directory Servers to Meet Entrust LDAP Requirements
- Completed Audit of CP, CPS and RA Operations
- Completed Technical Cross-Certification Between FBCA Prototype and NASA Development CA
- NASA Has Demonstrated Interoperability Between Its Developent CA and the Higher Education Bridge CA, Using the FBCA Prototype (either here or in current activities)

NASA PKI Current Activities

- Performing A Smart Card PKI Pilot Program
- Applying for Cross-Certification with the FBCA at Medium Level of Assurance
- Developing Secure Directory Server to Offload Pressure on NASA X.500 Directory Servers (?)
- Investigating Use of Roaming Profile
- Administrator Requested That Center Directors, Deputy Directors and Senior Management Be Able to Communicate Securely

NASA PKI Current Activities, cont.

- NASA Is Testing Interoperability Between The NASA Development CA and the Higher Education Bridge CA, Using the FBCA Prototype (either here or in recent accomplishments)
- NASA is Testing Entrust Version 6. Prior to Roll-Out Late in FY02

NASA PKI Next Steps

- Complete Cross-Certification with FBCA
- Incorporate PKI Into Integrated Financial Management System from SAP for Fall 2002 Deployment
- Integrate PKI With Electronic Forms Package
- Expand Smart Card PKI Pilot
- Modify NASA CP and CPS to Include Multi-Levels of Assurance
- Cross-certify NASA CA with Other CAs
  - Technical Support Contractors RSA Keon CA
  - NOAA CA?

NASA PKI Related Activities in e-Gov

- NASA CIO Chairs the CIO Council's Architecture and Infrastructure Committee
  - Has oversight of e-Authentication Initiative
- NASA Participates in the e-Travel Iniative
  - NASA will deploy GELCO Travel Manager as its single electronic travel system
  - NASA is working to integrate Travel Manager with the NASA SAP financial management software to enable travel related electronic accounting

NASA PKI Lessons Learned

- It Just Takes Time!
  - Estimate how much time it will take, then double it
- Spend Time to Educate Legal Staff
  - PKI is still new to your agency lawyers, they will be nervous
  - Keep Shauna's phone number and email address handy
- Set Your Requirements, Evaluate Against Them and Stick With Your Decisions
- Start Small with PKI and One or Two Apps
- Include Funding for Training in Your Plans
- Coordinate Your Plans With Agency IT Groups
- Make Change Management An Important Component of Your Roll-Out Strategy

NASA PKI Backup Slides

NASA PKI Procedure

- User contacts the Center Point of Contact (POC)
- POC gives user an application for a certificate
- User submits the application and gets trained
- User then gets initialization information after in person identity proofing by the Center RA
- Technical support people at the Center install the PKI software on the user's workstation
- User inputs the initialization information and receives their private keys

NASA Smart Card Requirements

- Provide two factor identification
- Support Entrust
- Support strong PINs
- Must be hack resistant (>8 char., upper & lower case alpha, numeric and special characters)
- Card infrastructure must be scalable
- Private key must not leave the card; must provide encryption and decryption on the card's processor
- Must support applications beyond PKI
- Must be standards compliant

NASA PKI Smart Card Pilot

- Performed Evaluation of Smart Card Products
  - Matrix of 16 smart card vendors against NASA requirements
- Selected Schlumberger Cryptoflex 32K Card
  - Wanted 32 K card, but Schlumberger was having trouble shipping them so settled for 16K card for pilot
  - ActivCard 2.0 Software
- Wanted Support for More Than Windows OS
  - ActivCard will write drivers for MAC OS, but funds are needed to support the effort