

Privacy Protection Protocols for Personal Security Devices

Eric Le Saint
Director of Security

May 2008

Actividentity™
DIGITAL IDENTITY ASSURANCE

Agenda

- ActivIdentity
- Privacy and Personally Identifiable Information
- Common Issues with Privacy
- Available Solutions: Privacy Protection Protocols
- A peek inside the protocols

ActivIdentity Profile



Company Profile:

- 315 Employees
- \$54M Rev / 27% Growth
- HQ Fremont, CA
- Development Centers in
 - United States
 - France
 - Australia
- Support Centers in
 - USA - California and Virginia
 - France
 - Canberra Australia

Vision:

Providing Government strength Identity Assurance to Employees, Consumers and Citizens, allowing people and organizations to electronically interact with confidence, anytime and anywhere.

Solutions:

Smart Employee ID (CMS, ActivClient)
Smart Citizen ID (CMS, ActivClient)
Strong Authentication (4TRESS, PKI and OTP tokens)
Enterprise Single Sign On
with secure Smart Card Credential Store
Integration with leading physical security systems

Keys to Success:

Strong Product Development, Delivery and Support
Direct Touch Sales Model
Contribution of Expertise to industry Standards initiatives
Intellectual property portfolio – over 200 patents
Solaris is a strategic, fully supported platform

Solutions at a glance

Strong Authentication

- Enables remote access, workstation & network access, application access
- Supports smart cards, one-time password & USB tokens, biometrics
- Improves security via two-factor authentication across the enterprise



Enterprise Single Sign On

- Automates access to virtually any enterprise application
- Supports shared workstations as well as individual workstations
- Improves both productivity and user experience



Smart Employee ID

- A smart card for both IT/logical access and facilities/physical access
- Replaces both security badges and remote access tokens
- Enables Strong authentication, single sign on, secure info & transactions



Secure Information and Transactions

- Create legally binding transactions with two-factor security
- Encrypt sensitive data or computers with two-factor security
- Supports smart cards, USB tokens and one-time password tokens



Personally Identifiable Information

- PII = Personally Identifiable Information
 - Elements of a digital identity
 - Allows the identification of a person or entity when combined with other PII
- PII Types
 - Globally unique identifiers: Social Security Numbers, Card Serial Numbers, Passport numbers, Certificate public keys, ..
 - Local identifiers which can be combined with local context information: account names
 - Secrets: PINs, passwords

When security meets privacy

- Today security is mostly targeted at protecting central resources or services or user credentials.
- The service requester has to release Identifiers in the initial steps of the service transaction
- So, the protocols expose PII (personally Identifiable Information) and specifically Global Unique Identifiers.
- Every time the personal security device is used, the attacker can potentially track/monitor usage.
- It is unavoidable that weak systems will use the PII in databases along with biographic, demographic data and the binding becomes accessible and vulnerable to improper use.
- When specific users are located, specific aggressive actions might be triggered.
- Security depends on privacy!

Privacy requires PII Protection in Personal Security Devices

- Disclosure of PII must be on a need to know only, and/or on authorization basis
- Protection during storage and transfer
- Forward secrecy.

Common Issues with Personal Security Device Applications

- PII storage protection
 - No Protected access from contactless interface
 - No Confidentiality protection
 - PII transfer protection
 - No confidentiality protection with contact and contactless
 - No Target or Requester Authentication and Authorization.
 - No Forward Secrecy:
 - Communications can be decrypted after transfer is completed
- Need security measures to enable privacy

How to protect PII transfer from Personal Security Devices

We consider a PSD including PII associated to the PSD owner.

4 steps

- 1) Optionally verify PSD owner's presence
 - 2) PSD authenticates, authorizes PII requesting entity,
 - 3) Optionally authenticate PSD to requesting entity.
 - 4) Then transmit PII to requesting entity with end-to-end confidentiality protection.
- Smart card serial numbers, certificates, access codes, Social Security Numbers are NOT transmitted in the clear between the application and the security device.
- **Benefits**
 - PSD owners cannot be tracked by attackers against their will.
 - PII of PSD owners cannot be copied and Digital identities cannot be impersonated

How to enable Forward Secrecy

- Use Forward secrecy technology to enhance confidentiality protection during PII transfers with Personal Security Devices

Benefits

- Even if:
 - 1) the attacker has captured PSD communication logs including PII protected for confidentiality,
 - 2) after the PII transfer has ended, the attacker manages to gain access to the static keys that were used to protect the transfer,
- The attacker will never be able to obtain the actual PII value.

Available Privacy Protection protocols

- Use end-to-end Secure channel protocol with mutual authentication, privacy protection and forward secrecy
- Existing solutions:
 - PLAID SKI/AES: (no forward secrecy)
 - Modular-Extended Access Control PKI/EC
 - Caernarvon/800-56 PKI/EC

Technology

- IPSEC/IKE
- Elliptic Curves (Suite-B)
- Diffie Hellman key agreement (w/EC)
- NIST 800-56A recommendations.

A peek inside the protocol

- Establish secure session between the PSD application and its client application using ECDH with ephemeral keys pairs on both sides, and producing session keys according to 800-56A.
- PSD authenticates client using a separate static client authentication key, and validate that the client owns both the ephemeral private key and the authentication key, to prevent a man-in-the middle attack.
- Client authenticates the PSD, in the same fashion, but the transfer of PSD identification data is protected with the session keys, and prove to the client that the PSD owns both the ephemeral private key and his static authentication key.
- Destroy all ephemeral keys when the transfer is complete.
- The channel is ready to transport any PII data back and forth with privacy and forward secrecy protection.

Actidentity Contributions

- Actidentity has contributed privacy protection protocol specifications to ISO 24727, ANSI (PIV+) and Global Platform Card Specifications.
- The privacy protection protocol specifications made by ActiVidentity are not subject to a license.

THANK YOU!

Eric Le Saint
elesaint@actidentity.com
+1 510 396 8871