

How Smart Cards Can Help Win The Digital Identity Challenge

Patrick George, Olivier Rouit

Gemplus

Overall Presentation Goals

- Introduce digital identity
 - Strong digital identity and authentication
 - The digital identity challenge

- Present relevant industry initiatives
 - Liberty Alliance (Liberty)
 - Trusted Computing Group (TCG)
 - Open Authentication Reference Architecture (OATH)

- Show how smart card contribute to these initiatives
 - Multi-factor authentication
 - Credential provisioning

- Discuss innovative solutions
 - Focus on OTP
 - Smart card and TPM complementarities

Digital Identity

- Identity (*Oxford English Dictionary*)
 - The fact of being who or what a person or thing is
 - The characteristics determining this
 - A close similarity or affinity
- Digital identity (*Phil Becker – Digital ID World*)
 - The representation of a human identity that is used in a distributed network interaction with other machines or people
 - Consists of two parts
 - The identity itself, i.e. who one is
 - The credentials that one holds, i.e. the attributes of that identity

Authentication

- Process that proves that the digital identity really represents who it says it does
 - To the level of trust required by the transaction involved
 - With an acceptably low risk of forgery

- The foundation of all security
 - The security of the system is only as strong as its weakest link
 - Authentication is the only aspect of security that must involve the user

- Issues
 - Many authentication mechanisms and many authentication authorities
 - Multiplying effect reduces security
 - Users must keep track of multiple identities
 - Organizations must keep track of multiple identities
 - Problems with issuing and revoking credentials for multiple authorities
 - Private authentication information need to be passed to each authority
 - Being authenticated in one location doesn't mean being authenticated in another location

Strong Digital Identity

- Strong digital identity
 - A digital identity thoroughly authenticated
 - Directly relates to the strength of the authentication method
- Strong authentication
 - “Everything but passwords”
 - At least 2-factor authentication
 - PIN/TAN
 - Token-generated One-Time Passwords (OTP)
 - Public Key tokens
 - Biometrics
- Motivations for stronger authentication
 - Emergence of federated networks
 - Regulation
 - Identity theft

The Digital ID Challenge

- Authentication is a major aspect of trust-based identity attribution
- One of the key challenge for organizations designing digital identity solution is provide authentication methods that
 - Lower the risk and costs associated with authentication
 - Tackle the identity credential provisioning issue
 - Ensure user privacy
 - Improve user convenience
- Many organizations are ready to take up the Digital ID Challenge
 - Liberty Alliance
 - Trusted Computing Group
 - OATH

Liberty Alliance

- Consortium developing open standards
 - For federated network identity management
 - For identity-based web services
 - Coordination with other standards groups

- More than 160 participating members
 - Government, business and consumer facing organizations
 - World-wide cross-section of organizations

- Develops open specifications that anyone can implement
 - Does not deliver specific products or services
 - 20+ Liberty-enabled products and services available

Federated Network Identity

- Federated Network Identity involves
 - Account federation
 - Federated single sign-on

- Account federation enables binding a user's multiple accounts within an affiliated group
 - Established between commercial and/or non-commercial organizations
 - Governed by some legal agreement

- Federated single sign-on enables users to
 - Sign-on with one member of an affiliated group of organizations,
 - Subsequently uses other sites in the group without re-authentication

Liberty Contribution

- Federated Network Identity
 - Supply superior security, control, and privacy-improving trust
 - Provision accounts and securely provide access to designated resources both within and outside corporate borders
 - No single point-of-failure
 - Eliminate excess passwords and securely implement single sign-on
 - Improve authentication with existing internal resources
 - Reduce risk through a more balanced authentication process

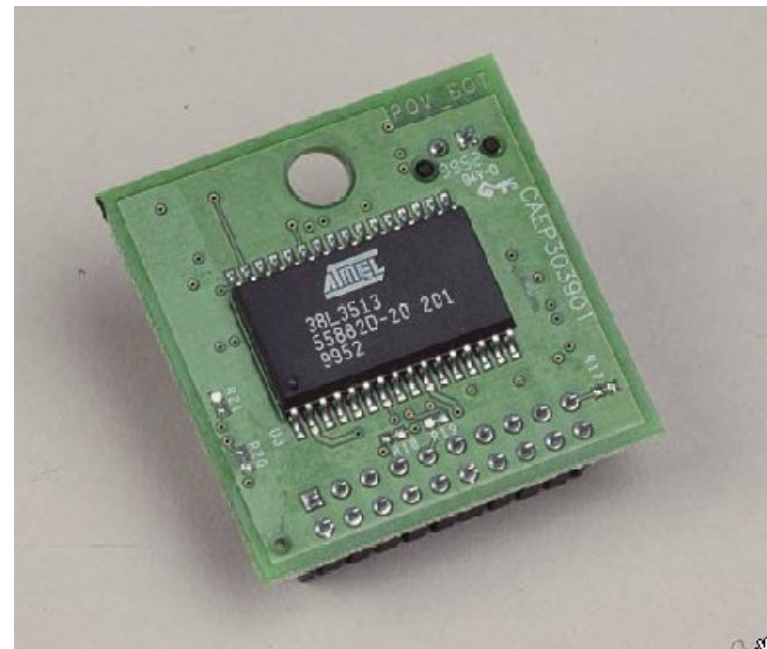
- Federated authentication
 - Disparate mechanisms joined into a single, logical whole
 - May be different types

Trusted Computing Group

- TCG develops and promotes open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms
- TCG is incorporated as a not-for-profit corporation, with international membership
 - Open membership model (110 members)
 - Offers multiple membership levels: Promoters, Contributors, and Adopters
 - Board of Directors
 - Promoters and member elected Contributors
 - Typical not-for-profit bylaws
 - Industry typical patent policy (Reasonable and Non Discriminatory) for all published specifications
 - Working Groups

Trusted Platform Module

- A silicon chip that performs all TPM v1.x functions, including:
 - Store platform integrity measurement
 - Generate and store a private key
 - Hash files using SHA-1
 - Create digital signatures
 - Anchor chain of trust for keys, digital certificates and other credentials



TCG Contribution

Unique Platform Authentication

- Eliminates platform spoofing
- Higher level of assurance within the security realm

Privacy

- TCG TPM specification incorporates current privacy principles
- User controls TPM secrets
- TPM secrets used to protect user identity and information

HW protection of sensitive data

HW-protected Storage

- Mitigates risk and liability from stolen or copied certificates
- Ensure that personal data will not be compromised
- Protects all sorts of sensitive data

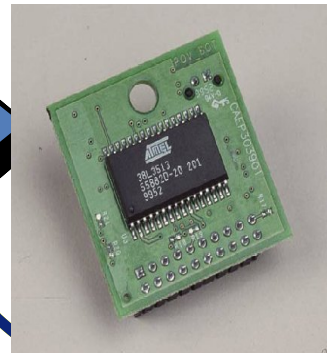
Authentication

Privacy

Convenience

Reduced Cost and Administration

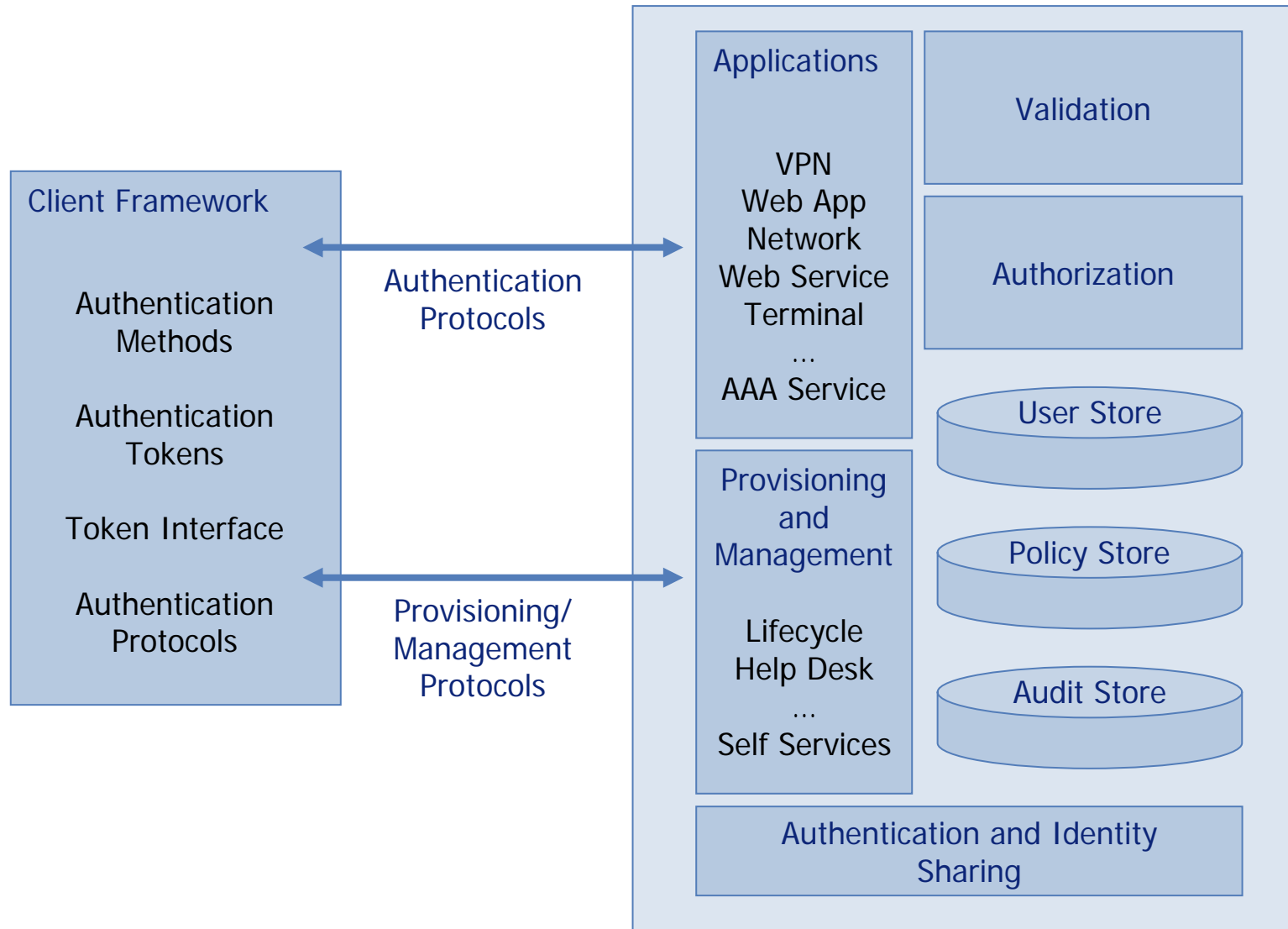
- Provides the HW functionality of portable tokens needed for remote access authentication



OATH

- The Initiative for Open Authentication (OATH) is a collaborative effort of IT industry leaders aimed at providing a reference architecture for universal strong authentication across all users and all devices over all networks
- More than 50 participating members
 - Device manufacturers (chips, smartcards and tokens)
 - Application developers (PKI, VPN, ...)
 - Platform vendors
- It is now a RFC going for ratification at IETF

Authentication Framework

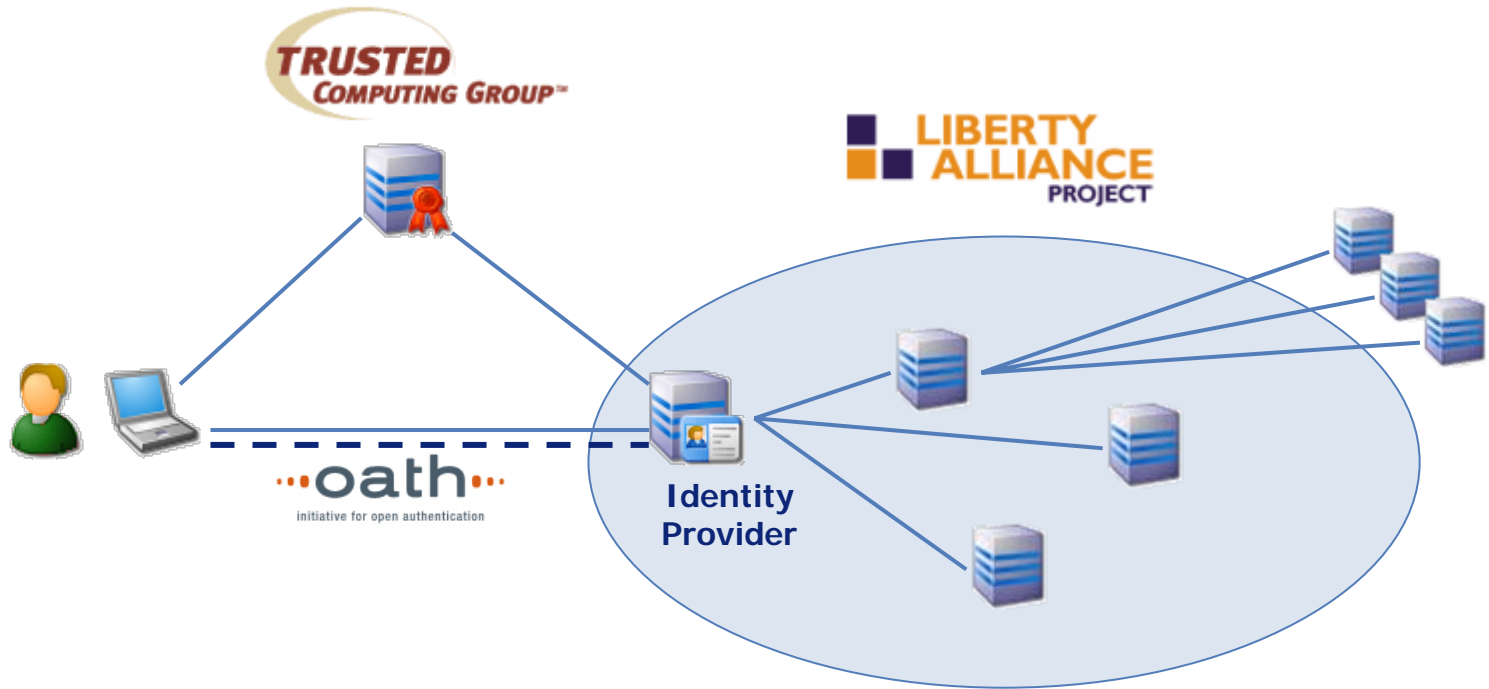


OATH Contribution

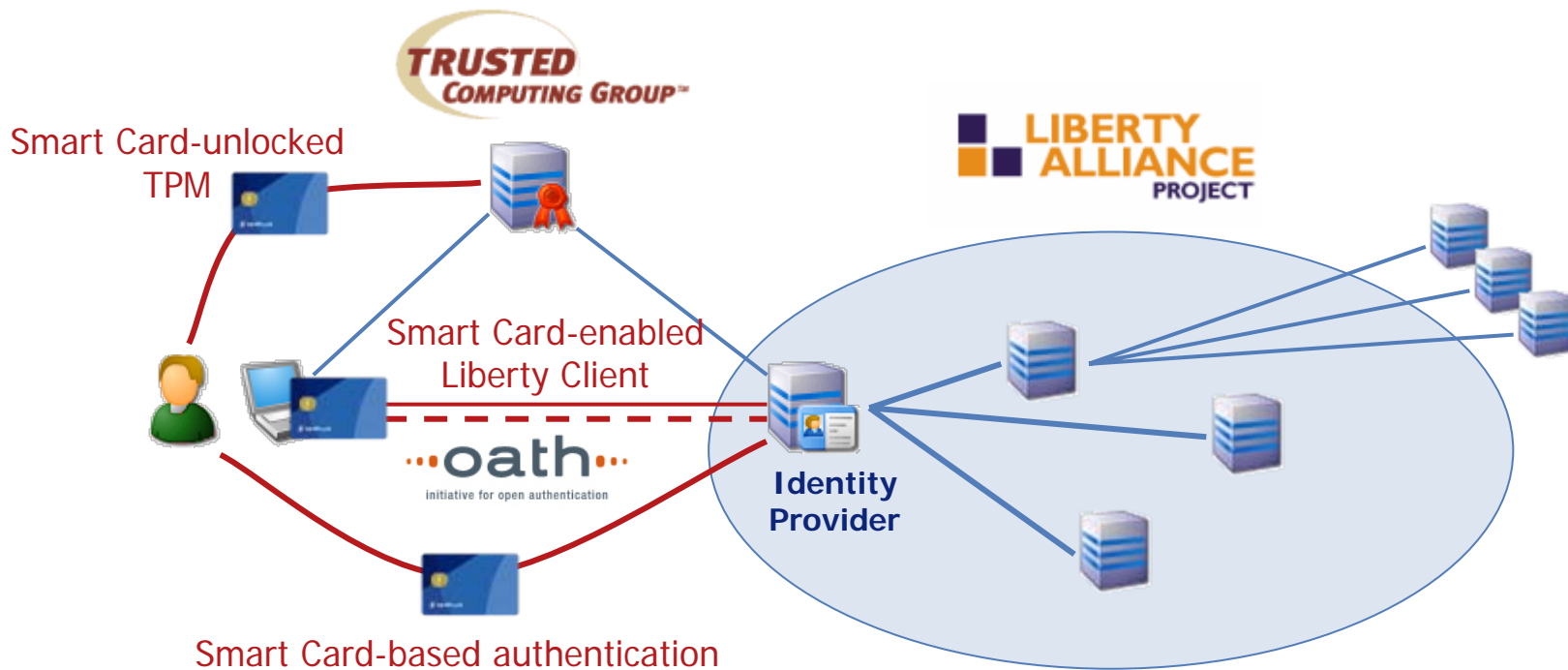
- A common framework for the strong authentication of users and device

- The key guiding principles behind the Reference Architecture include:
 - Open and royalty-free specifications for strong authentication
 - Device innovation and embedded specified technology building blocks for strong authentication
 - Native platform support
 - Interoperable modules that enable best-of-breed hardware and software solutions through a framework of interoperable components

The Big Picture



Where Do Smart Cards Fit?



Smart Cards In Liberty

- Smart card protects identity credentials
 - Performs the authentication method
 - PIN protected
- Liberty Intelligent Client specification supports smart cards
 - Define identity management mechanisms where the user device has enhanced capabilities
 - Provide services even if the device is offline
 - Allow web services across a variety of devices
 - Expand the opportunity for additional types of strong authentication mechanisms
 - Smart cards
 - SIM devices
- Smart cards can hold identity attributes

Smart Cards In TCG

- Does one security device fit all?
 - Same device for platform and user secrets?
- Separate credentials
 - User credential portability
 - User administration simplification
 - Protection level adequacy
 - User privacy
- Leverage from corporate deployments
 - Logical access to computers
 - Physical access control badges too
- Toward a smartcard-and-TPM cooperative model

A First Application

- The TPM user must be authorized before using TPM-protected resources
- User authentication is based on the proof of knowledge a secret shared between the user and the TPM
- This method raises security concerns
- A smart card can be used to perform user authentication without exposing the Authorization Data



Smart Cards In OATH

- Smart card protects identity credentials
 - Store identities
 - Generate the authenticator (e.g. One-Time-Password)
 - PIN protected
- Different form factors are available
 - Smart card (ISO or plug-in)
 - SIM card in a Mobile
 - STK applet
 - Bluetooth connection
 - USB token
 - Off line generation
 - PC connected
 - MMC card with Smart card ability (XMC)

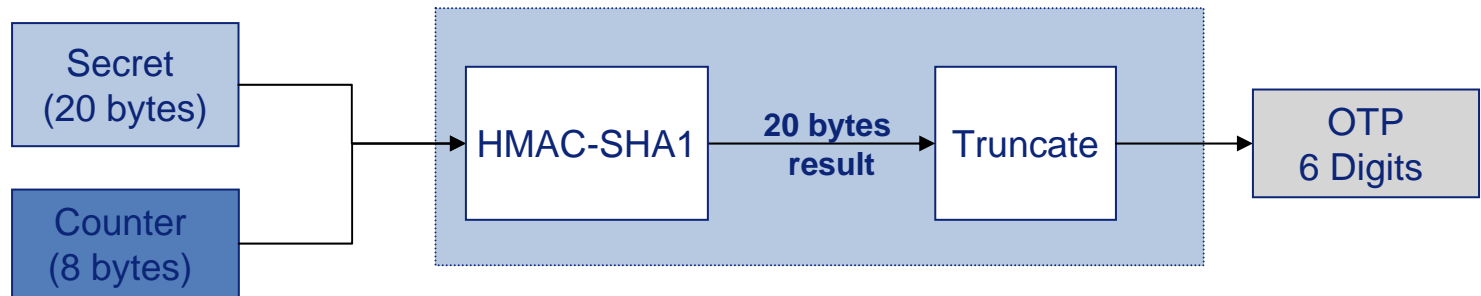


An OATH-based Solution For MNOs (1)

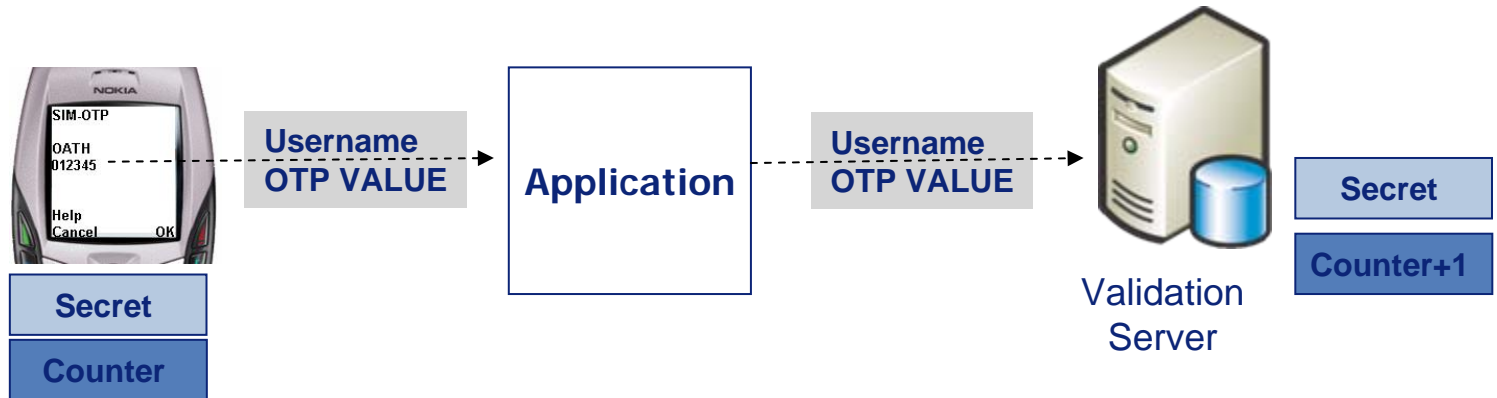
- A SIM card performs the authentication algorithm
- The handset is used as a hardware secure token to remotely activate/deactivate the application over cellular networks
- Implements a One-Time Password (OTP) algorithm based on
 - HMAC-SHA1 a FIPS standard hashing algorithm with no known hashing weakness
 - The IETF defined truncation algorithm that extracts the 6 digits from 20 bytes intermediate result
- SIM and validation server are provisioned with the same seed
- The token computes the next OTP as follows
 - Counter = Counter + 1
 - OTP = Truncate(HMAC-SHA1 (Counter, Secret))

An OATH-based Solution For MNOs (2)

- Generation



- Verification



Conclusion

- Authentication is a major aspect of trust-based identity attribution, and smart tokens are ideal authentication devices
 - Provide multi-factor authentication
 - Tamper-resistant
 - Implement various authentication methods
 - Allow secure provisioning of identity credentials

- The industry supports initiatives that provide digital identity building blocks
 - Liberty for federated identity framework
 - TCG for platform security
 - OATH for authentication framework

- Smart cards are the link between these initiatives
 - From simple authentication token
 - To sophisticated security enhancer
 - TPM security companion
 - Identity attribute server