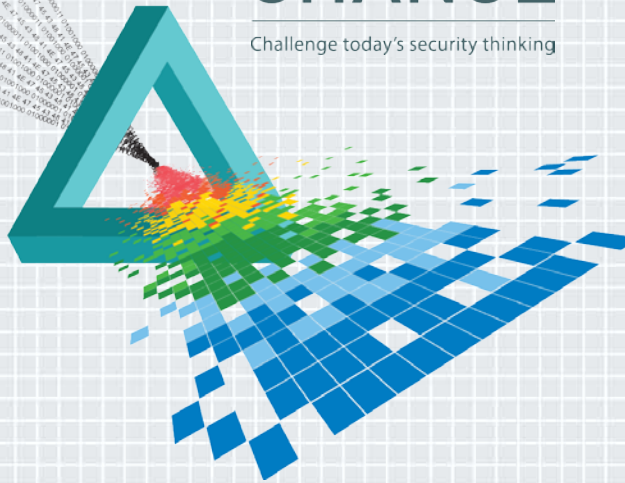
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: IDY-R02

Identity Proofing – Blinding the Eye of Sauron

Paul Grassi
Senior Standards and Technology Advisor
National Strategy for Trusted Identities in Cyberspace, National Program Office
National Institute of Standards and Technology

Chi Hickey
Manager, Trust Framework Provider (TFS) Program
General Services Administration

Identity Proofing 101

- A process that vets and verifies the information (e.g. identity history, credentials, documents) that is used to establish the identity of a system entity
- Considerations
  - Remote vs. In-Person
  - Document collection and verification
  - Required data elements
  - Personally identifiable information
  - Maintenance and protection of information

Identity Proofing Components

- Identity Resolution

- Identity Validation

- Identity Verification

Identity Resolution

- Uniquely distinguishing an individual from all other people in a given context
- Requires
  - Collection of attributes
  - Minimal amount of data that allows uniqueness to be determined
  - Consent to use attributes

Ensures that the smallest set of attributes have been resolved to a unique individual in a given population

Identity Validation

- Establishing the accuracy of the identity information via:
  - An authoritative source
  - Corroborating different sources of information if no single authoritative source is available

Ensures that identity information is accurate and timely

Identity Verification

- Confirming that the identity information provided relates to a specific individual

Ensures that the identity information is not being fraudulently used

Identity Proofing Methods

Remote Proofing			
Pros	**Cons**	**Resolution**	**WEAK**
Convenient	KBA Risk	**Validation**	**WEAK**
Low Cost	Easy impersonation	**Verification**	**WEAK**

In-Person Proofing			
Pros	**Cons**	**Resolution**	**STRONG**
High resolution	Inconvenient	**Validation**	**Medium**
Availability of biometrics	Costly	**Verification**	**Medium**

Where Does This Put Us?

- ID Proofing is still a challenge for many organizations
- Every organization is doing it themselves
- Users are proofed multiple times
- Your Proofing! = My Proofing
- Customers are increasingly concerned about their privacy
- Federated environments are decreasing the number of stores of identity information
- Hub architectures are reducing the barrier to federated identity

Federated Identity vs Hub Solution

Current State

- Requires agencies to integrate with multiple Identity Service Providers (IDPs), each independently paying for authentication services
- Limited LOA 2 & 3 credentials due to limited demand

The Solution (Connect.Gov)

- Centralized interface between agencies and credential providers – reduces costs and complexity, speeds up integration timeline for new IDPs
- Enhanced consumer privacy and experience; user does not have to get a new credential for each agency application
- Decreased Federal government authentication costs

But...

So What Are We Doing?

- Reviewing ways to establish and authenticate identity
  - Recent technology development
  - Failures in remote proofing
- October 17, 2014 Executive Order Implementation Plan
- Focus on identity proofing and identity assertions that are strong, reliable, and privacy enhancing
- NIST SP 800-63 released for review/comments:
  - http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2_call-comments.html

How Are We Building It?

Meaningless But Unique Number (MBUN)

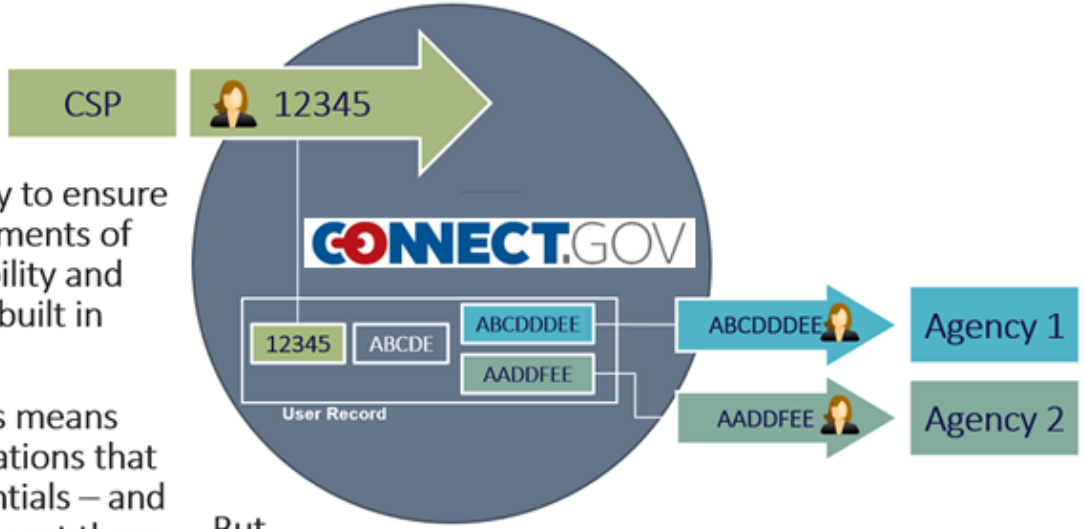
- Unique among the CSP's and users
- Protocols use an anonymous value as a requirement for the Subject
- Used to describe the value provided by CSPs as the Subject of the Authentication Response
- Specified by CSP

Persistent Anonymous Identifier (PAI)

- NOT derived from MBUNs
- Created with the Java SecureRandom class
- Stored with MBUNs = Mapping
- Generated by Broker
- ID Broker Store: MBUN, iPAI
- Federation Manager Store: iPAI, rpPAI

Privacy By Design

- Designed specifically to ensure that privacy requirements of anonymity, unlinkability and unobservability are built in from the start
- In simple terms, this means that private organizations that issue citizens credentials – and the agencies that accept them – will have no way to track where citizens use them.



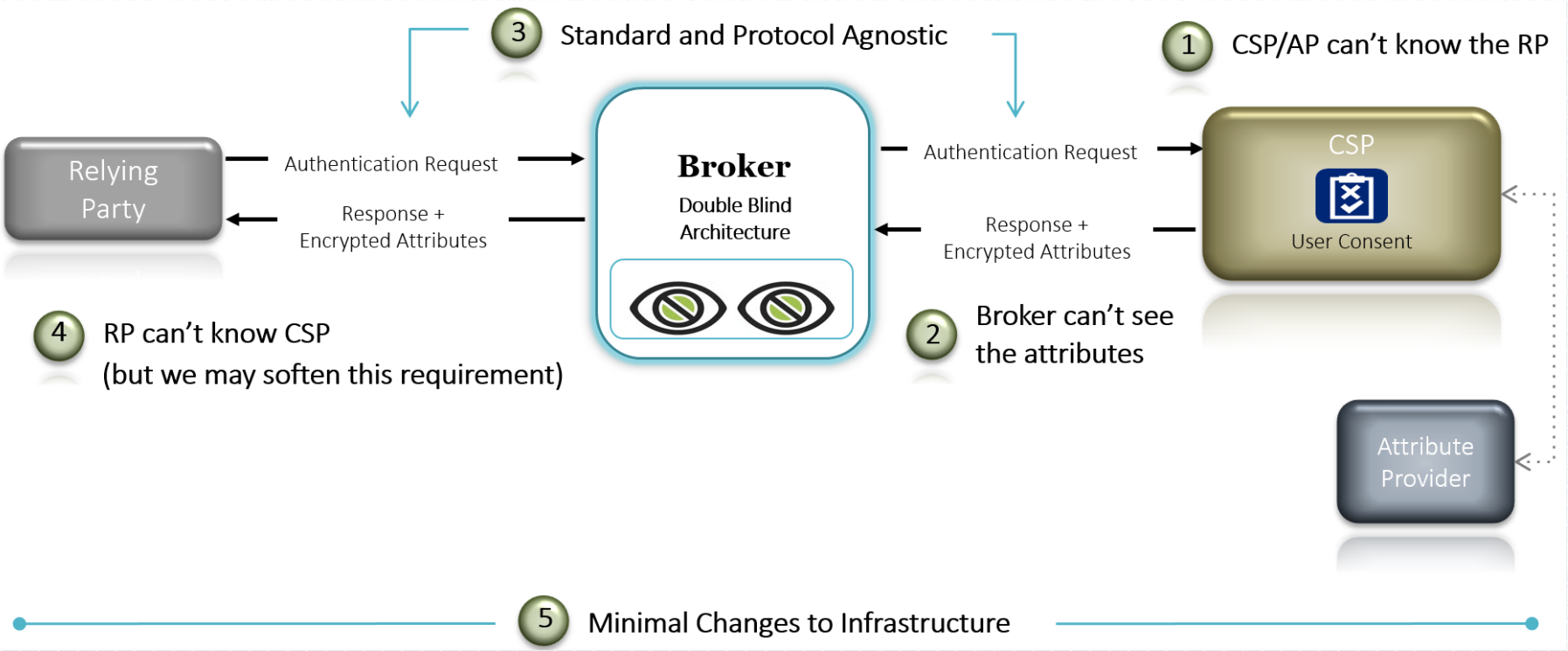
But…

- Attributes flow freely through FCCX
- If they didn't, RP's would get them on their own (inconsistently)
- "Let the RP Figure It Out" is the wrong answer!

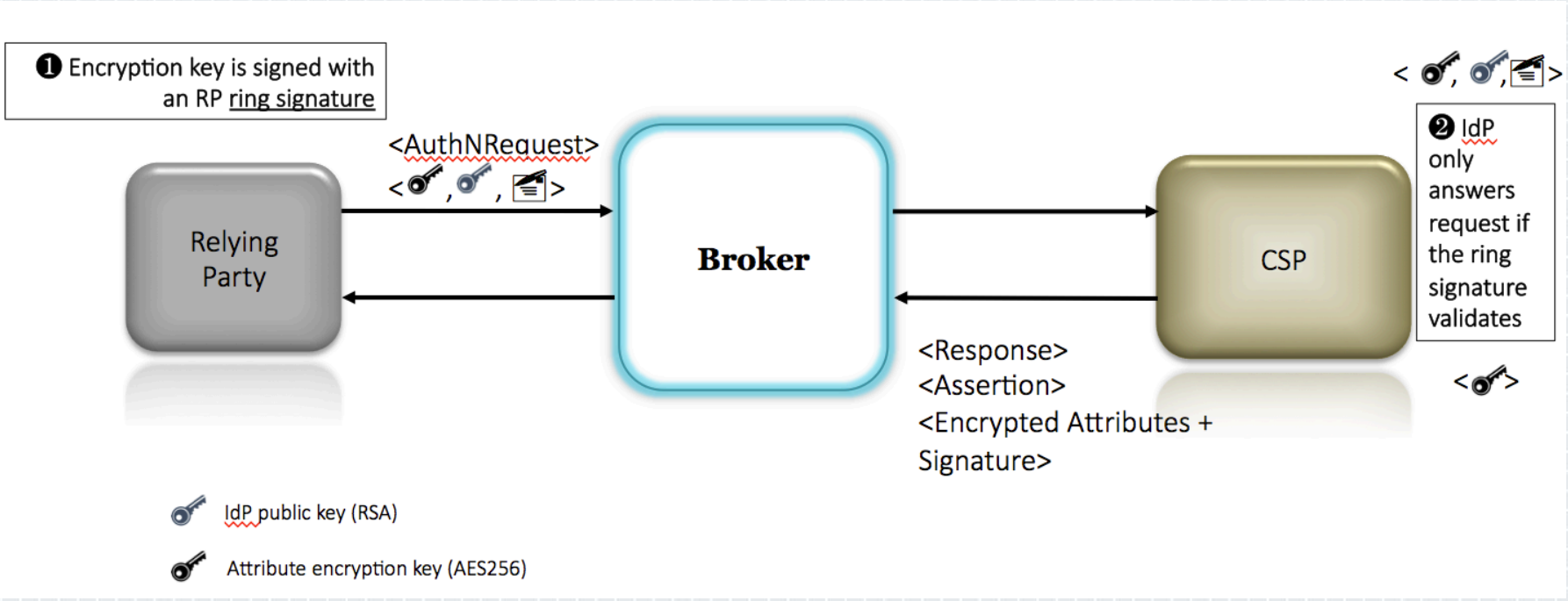
There Is More To Do

- Broker infrastructure has access to attribute values sent from CSPs
- Identity protocols are based on explicit trust and knowledge of endpoints
- Encryption and signing requires knowledge of public keys = no longer blind
- Attributes are not persisted, but in-memory processing is an attack vector for malicious actors
- Double Blind is OK for data-at-rest, but not for data-in-motion
- Attribute Encryption is not enough, risk remains where the Broker is Honest-But-Curious, enforced only through policy. A malicious actor can bypass these controls and obtain read/write access to attribute data.
- Impersonation Attacks

A Desired Hub Architecture



And A Potential Secure, Privacy Flow



Summary

- Identity Proofing
  - Identity Resolution
  - Identity Validation
  - Identity Verification
- Minimize the amount of data collected
- Address privacy concerns
- Leverage hub architectures

Applying the Blinders

- Analyze identity proofing requirements and the level of risk associated with what is being protected
  - Are they commensurate?
- Identify extraneous identity proofing requirements
- Pinpoint critical data that may be targeted – Avoid honeypots
- Implement mitigating elements, surveillance tools
- New standards and profiles
- Updated cryptography APIs
- Increased market adoption

Questions?