

# Anonymous Credentials

Feb 15, 2013

# Anonymous Credentials

- Allow a person to make trusted assertions in response to Policy Questions (eg are you older than age 21, do you have a valid Driver's license, etc ?)
- ...while minimizing information release and leakage (eg YES, but I will not tell you my DOB or my Name)

# What are Anonymous Credentials ?

- Derived from Assertions by trusted Identity Providers
  - Eg bank, government, employer, K12 school system, etc.
- Trusted Assertions can satisfy access policy requirements of Service Providers
  - Implementations support user control of release process
  - Crypto evidence supports validity of claim
  - Optionally revealing the values from the original Assertion

# Properties of Anonymous Credentials

- Tamper-proof; protected by standard PKI
- non-transferable; linked to a specific user
- Crypto validation of claims
- SP can validate the chain of trust to the Issuer
- SP can detect revocation of original credential
- Inspector process (governed by law and (inter?)national policy) can potentially look inside Anonymous Credentials

# History of Anonymous Credentials

- Stefan Brands
  - Credentica; Microsoft - uProve
- Anna Lysyanskaya
  - IDEMIX; Implementation by IBM Zurich Lab
- Commercialization failed; now open source
- Often described as very cool technology in search of use cases
- Were way ahead of their time; can now leverage other Internet identity infrastructure

# Many Privacy/Secrecy benefits

- Minimal disclosure - able to address policy requirements with yes/no answers, without revealing PII (anonymity)
- Selective disclosure - user decides which credential to use as basis, and what information to release
- Issuer does not know when the credential is being used(unobservability)
- Relying party can't correlate info received on multiple queries(unlinkability)
- Multiple relying parties can't correlate answers to track and correlate (unlinkability)

# Sample Use Cases

- Is the user associated with this token over 18? (legal age)
- Is the user between 11 and 13? (entrance into COPPA-compliant sites)
- Certified address provided to online merchant, for sales tax purposes
- Does the user have a security clearance of level at least X?
- The holder of the token is a certified first responder with special training in a specified set of skills
- Rent a car; prove that the user has a valid license, driver's insurance, and age > 25. Contents opened ONLY if car is not returned or user has an accident.
- The holder of this token is a registered citizen, living in a specific precinct, with permits issued for activities such as parking/shared cars, zoning exceptions, etc.

# Sample Use Cases

- Is this user a member of a group, or possess an Affiliation (eg student) that is eligible for a discount?
- Is the user associated with this attribute a resident of a specific dorm?
- Does the holder of this attribute attend University X?
- With your paper diploma and your identity-rich e-transcript, you get issued an anonymous token asserting affirmation of graduation and degree, year, honors, major
- Secret or private clubs (Is the holder a club member)
- The holder of this credential has this set of allergies
- User purchases an item at an online merchant, provides shipping address which cannot be seen by merchant but is forwarded to shipping company.



# How Does it Work ?

- Trusted Identity Providers give each User traditional PKI-based credentials
  - Eg bank, government, employer, K12 school system, etc.
  - Each certificate may contain multiple traditional attributes (eg name, DOB, address, certifications, etc)
- User will have multiple credentials

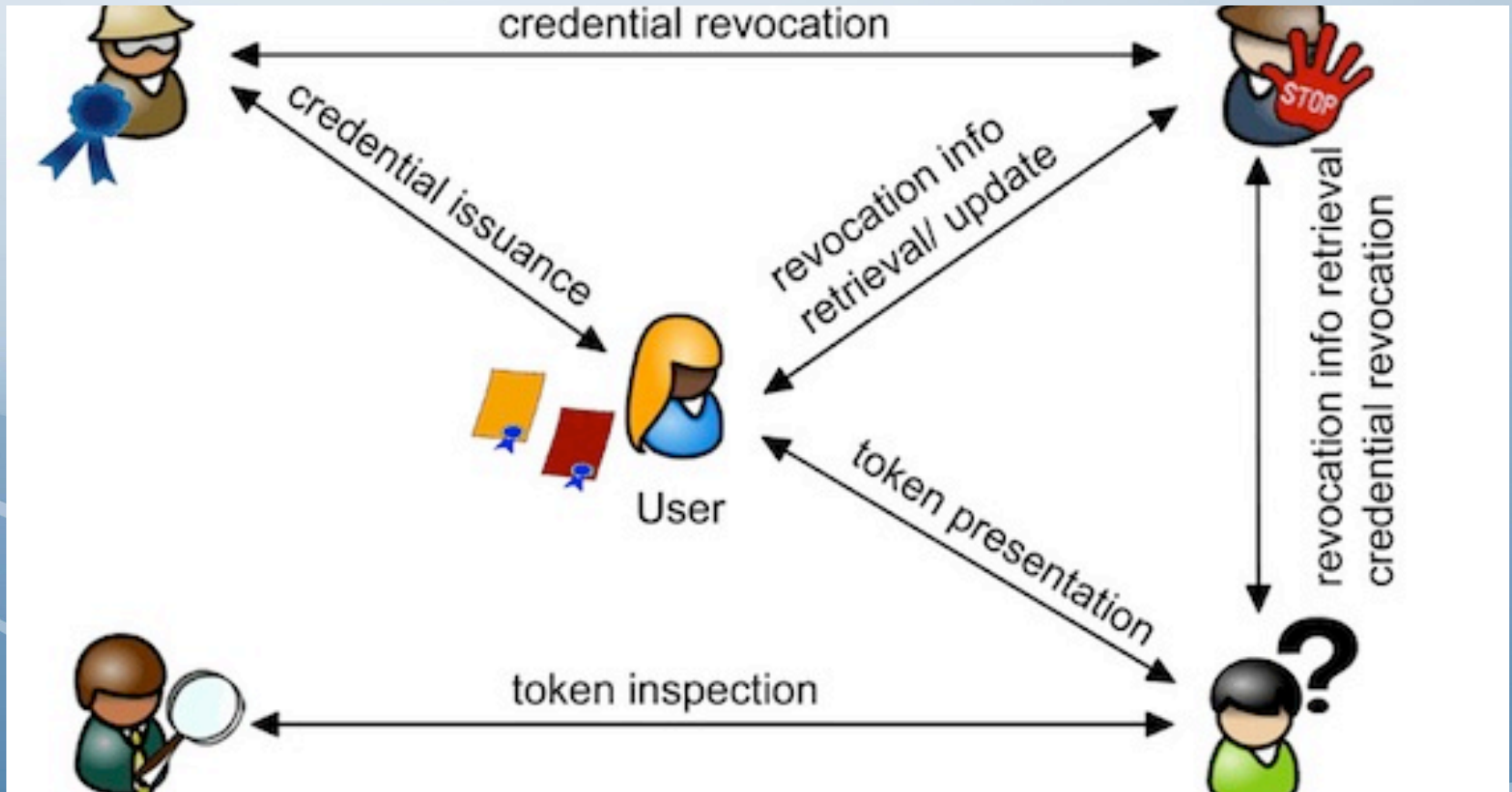
# How Does it Work ?

- SP' s Access Policy specifies requested information (eg age > 21; possess specific certification; etc)
- For each Policy request, user is presented with a list of credentials which can be used to satisfy the request; user chooses which one to use
- Presentation Tokens produced from original credential
  - Contains Assertions DERIVED from original attributes
  - Crypto evidence to support validity of claim (eg AGE > 21, rather than DOB)
  - Optionally contains the actual values
  - Even tho Presentation Token is derived and produced in the user' s desktop, SP can still validate the trust chain
- Presentation Tokens forwarded to SP, user gains access

# Presentation Tokens

- Can satisfy access policy requirements of Service Providers
  - Without necessarily revealing the values from the original Assertion used to create the Anonymous Credential
  - Does contain identity of the Identifier Provider which provided the original credential
  - SP can validate the chain of trust
  - SP can detect revocation of original Assertion
  - Inspector process (governed by law and (inter?)national policy) can look inside Anonymous Credentials
    - Info sealed with Inspector's public key

# Abc4trust flows




Kids-Chat.com - a hypothetica x

caldaro.zurich.ibm.com/kids-chat/entrance.html

### Claim Selection


Option 1

— ICard



Option 2


— MemberShipCard



OR

Option 2

— MemberShipCard



**Adapted Card**

**Revealed ownership:**

- ICard from Republic-Online.info.
- MemberShipCard from Kids-Chat.com.

**Revealed facts:**

- expirationDate of your Identity Card is after 2011-10-19.
- expirationDate of your Kids Chat Membership Card is after 2011-10-19.
- dateOfBirth of your Identity Card is after 1994-10-19.

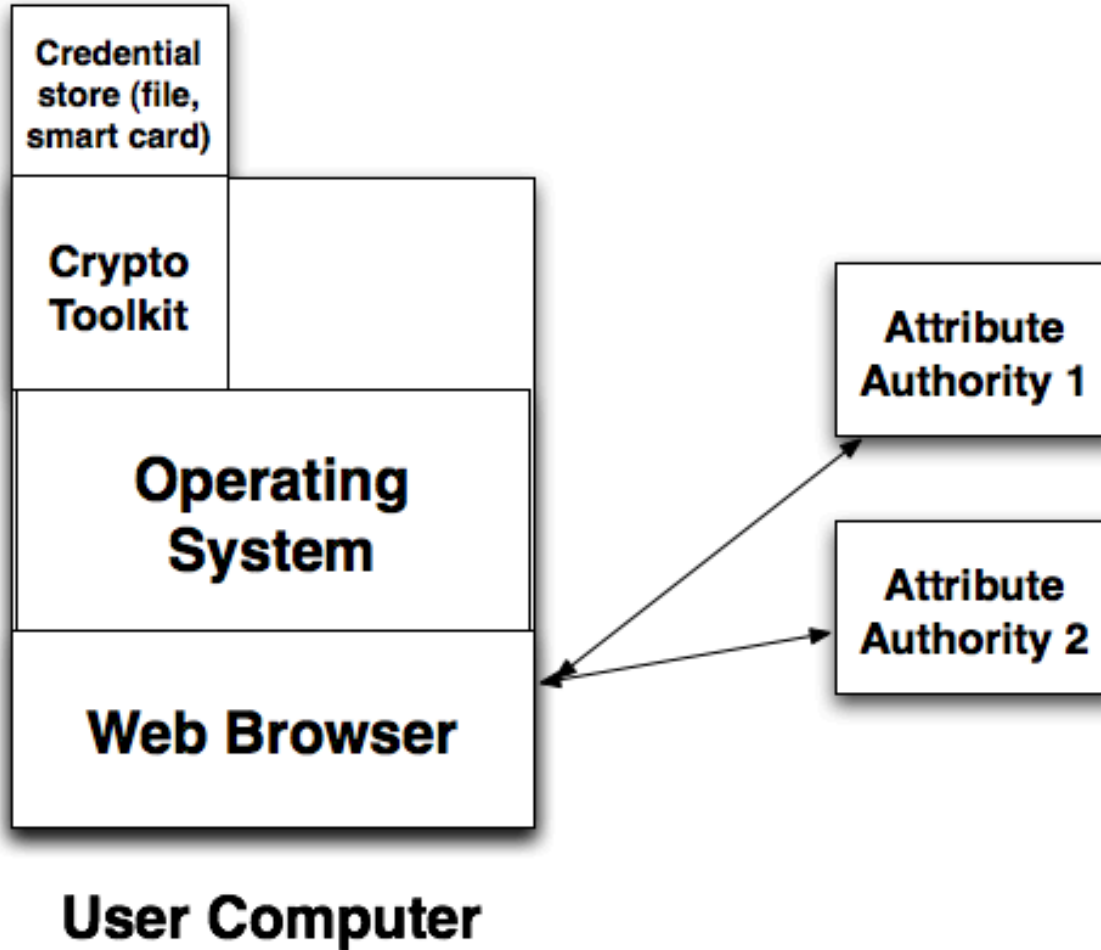
**Submit**

To use this site, you must have at least one valid Identity Mixer© credential. Most likely you got such a credential from your school. If you did not, you may ask your parents to

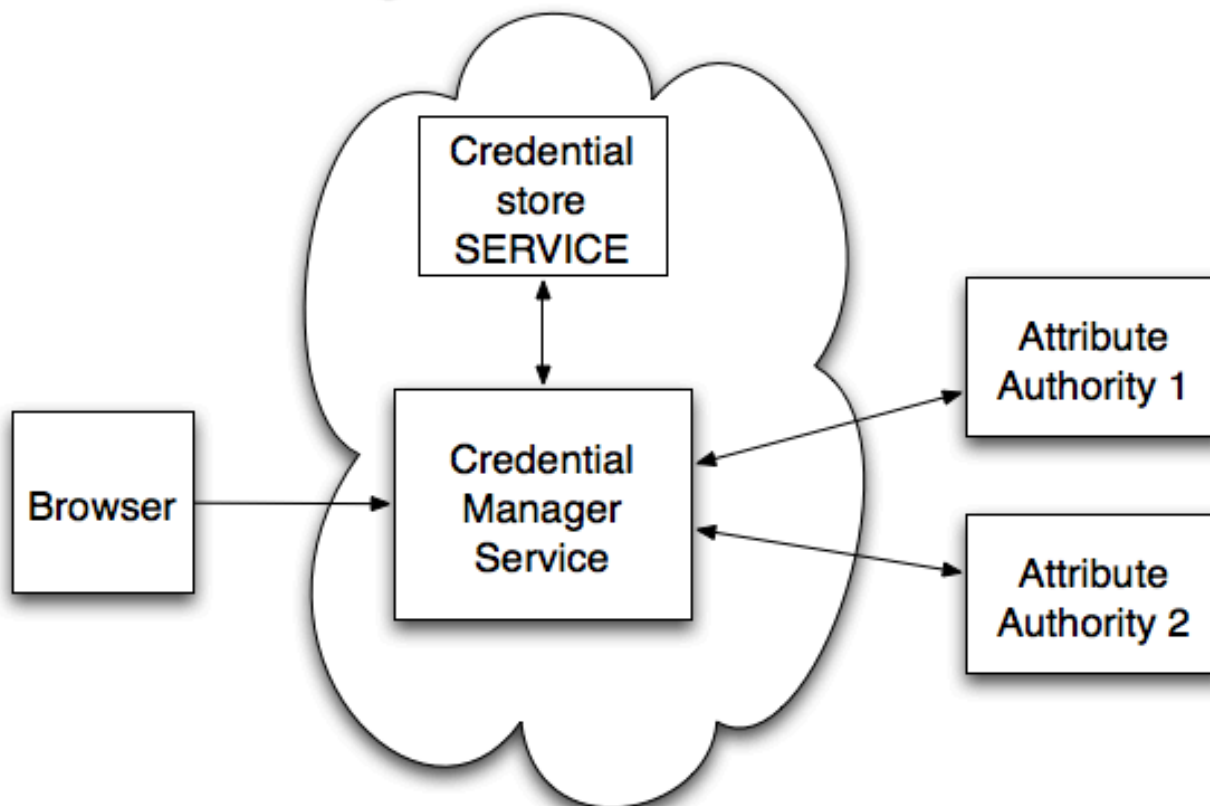
# Deployment Models

- Classic abc4Trust, Idemix, etc.
  - Credentials held in a cert store on the user's desktop or smart card
  - RPs accessed via Web Browser
  - Processing done in User's desktop by previously downloaded plugins
- Enterprise-based
  - Credentials held in enterprise directory
  - Processing still done in desktop
  - Addresses mobility
  - May serve important enterprise needs
- Cloud-based
  - Processing and storage moved to the cloud
  - Addresses mobility issues

## Obtaining Credentials - abc4trust

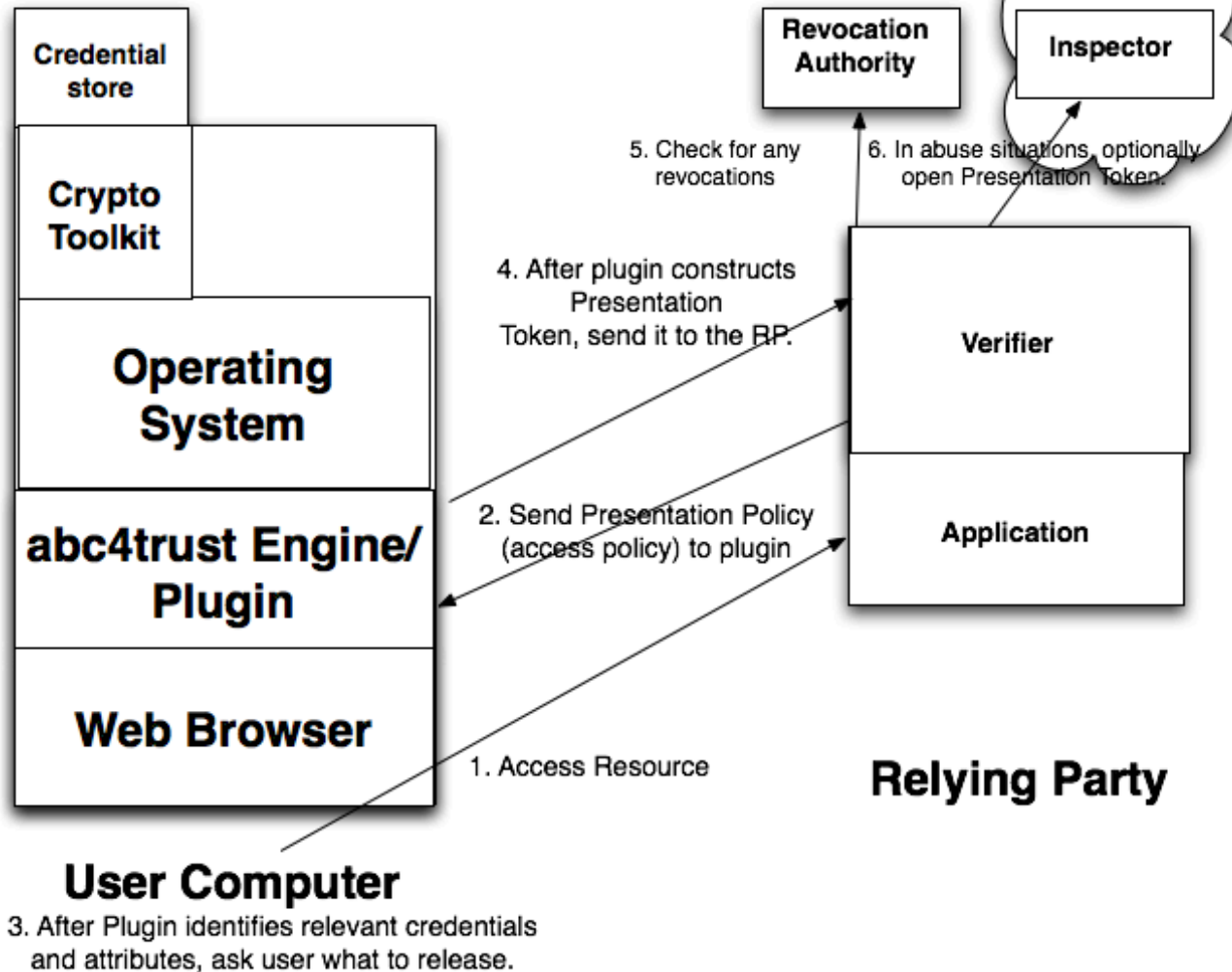


## Obtaining Credentials - New Model





## Access Resource -- abc4trust



# Criteria to Evaluate Technologies and Deployment Models

- leakage -- how are the original credentials protected from prying eyes? Are the credentials stored physically near or far from the user ?
- tamper-proof -- once an Identity Provider has issued a Credential, can alterations be detected by an SP ?
- non-transferable -- can a Credential be linked to a single user
- Anonymity -- can a credential be used without disclosing that user's Identity or Identifiers
- unobservability -- can the assertions/tokens be used without the IDP knowing where they are being used ?

# Criteria...

- unlinkability -- can an SP determine that a set of tokens or assertions presented over a period of time in separate transactions are associated with the same user ?
- minimal disclosure -- can the user produce trusted presentation tokens with the minimal required information (eg age > 21) without releasing the information used to produce that token (eg birthdate)
- informed consent -- can the user control which attributes and values are released to the SP ?
- Purpose Specification -- can the user see the Privacy Policies and Certifications (eg COPPA compliant) of the SP, and its intended use of the Attributes, before agreeing to release ?
- leakage -- what are the various ways that an SP can collect info about a user (eg browser IP address)

# Criteria ...

- mobility of tokens -- can the user easily use their tokens from different machines, different types of devices (eg laptop, tablet), different locations
- Data Quality and Integrity -- can the RP verify that the provided attributes are accurate and complete ?

# Deployment Issues

- Managing trust between parties (bilateral, federation provided metadata)
- Handling revocation issues
- Functional and usable User Consent Tools
  - UI issues
  - What \*really\* is Informed Consent ?
  - “Tell me more” functionality (purpose specification)
  - Out-of-band Consent
- Issues associated with Delegated use.
- Assessing privacy exposures of various models
- Minimizing the potential for Privacy Spills

# Next Steps (3 months)

- Expand use case registry
  - Refine existing
  - Request IDESG input
- Obtain, build, and evaluate abc4trust software
- Begin conversations with Microsoft/uProve
- Begin to identify issues associated with Enterprise deploy
- Begin conversations with campus experts

[www.internet2.edu](http://www.internet2.edu)

