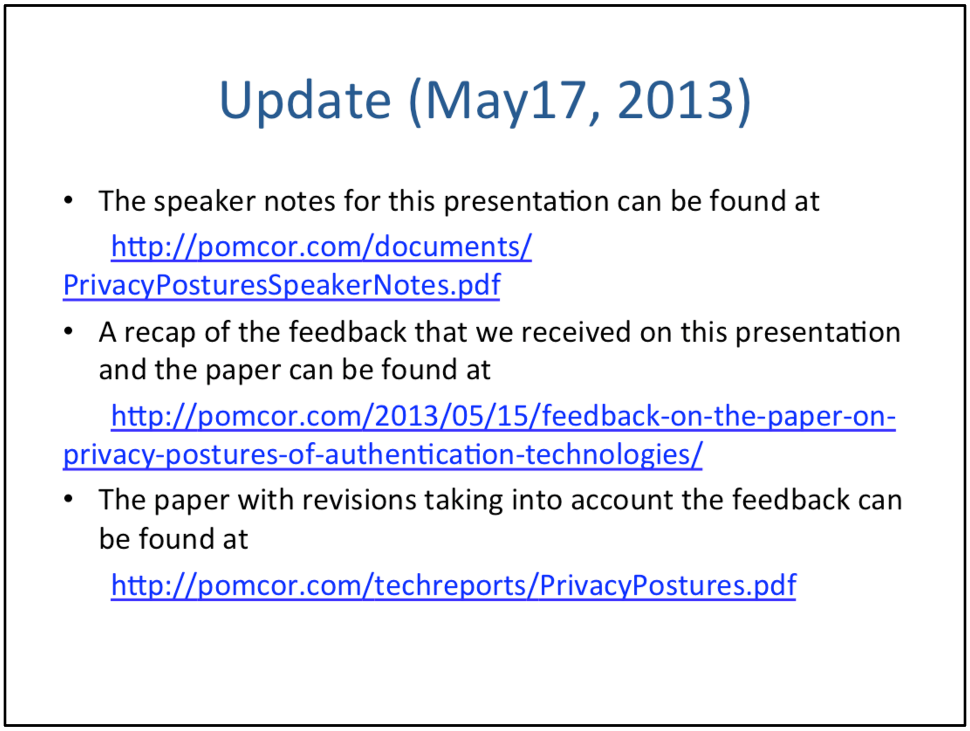
Privacy Postures of Authentication Technologies

Presentation to ID360 2013

Francisco Corella (fcorella@pomcor.com)
Karen Lewison (kplewison@pomcor.com)
Web site: pomcor.com
Blog: pomcor.com/blog

pomcor
pomcor.com



Update (May17, 2013)

- The speaker notes for this presentation can be found at

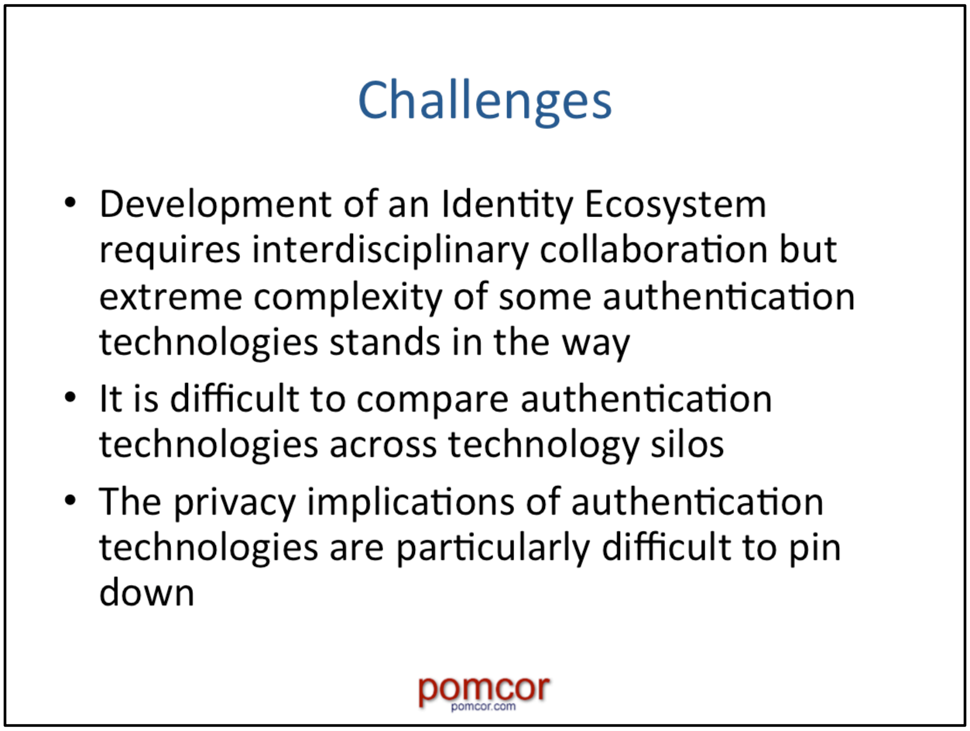
  http://pomcor.com/documents/PrivacyPosturesSpeakerNotes.pdf

- A recap of the feedback that we received on this presentation and the paper can be found at

  http://pomcor.com/2013/05/15/feedback-on-the-paper-on-privacy-postures-of-authentication-technologies/

- The paper with revisions taking into account the feedback can be found at

  http://pomcor.com/techreports/PrivacyPostures.pdf

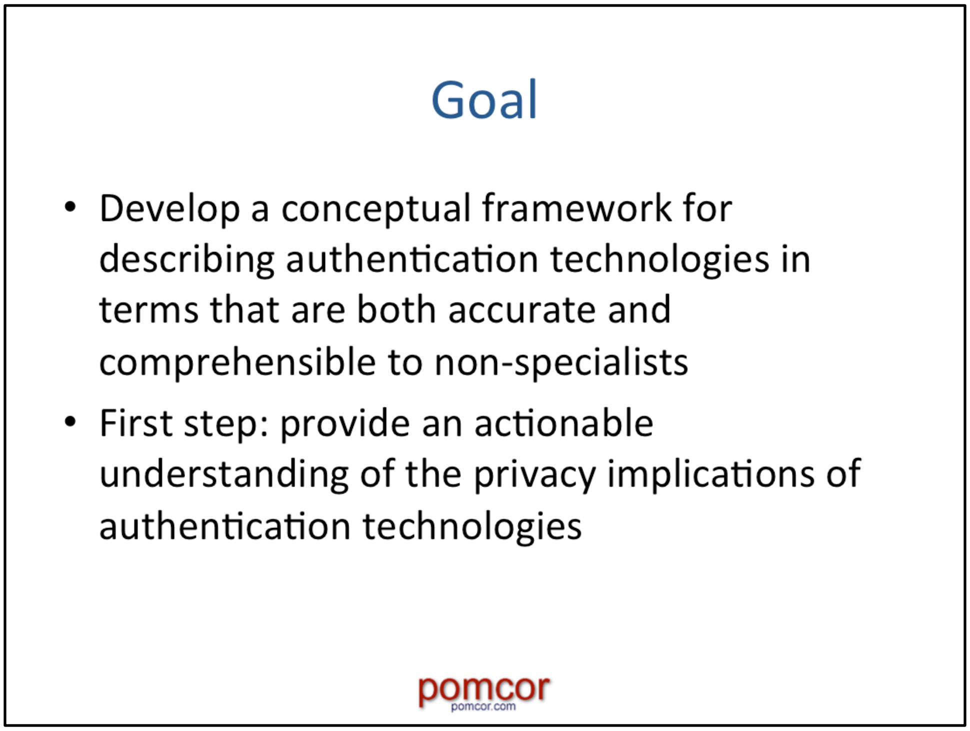


Challenges

- Development of an Identity Ecosystem requires interdisciplinary collaboration but extreme complexity of some authentication technologies stands in the way
- It is difficult to compare authentication technologies across technology silos
- The privacy implications of authentication technologies are particularly difficult to pin down

pomcor
pomcor.com

A theme of this conference is that the development of an Identity Ecosystem requires interdisciplinary collaboration.
In this talk I'm going to address one obstacle that stands in the way of effective collaboration,
namely the complexity of some authentication technologies, which makes them difficult to understand for experts in other disciplines.
Actually there are several silos within authentication technology, and experts in one silo do not necessarily understand the technologies in other silos,
which makes it difficult to compare technologies across silos.
In particular, the privacy implications of the many different authentication technologies are difficult to pin down.



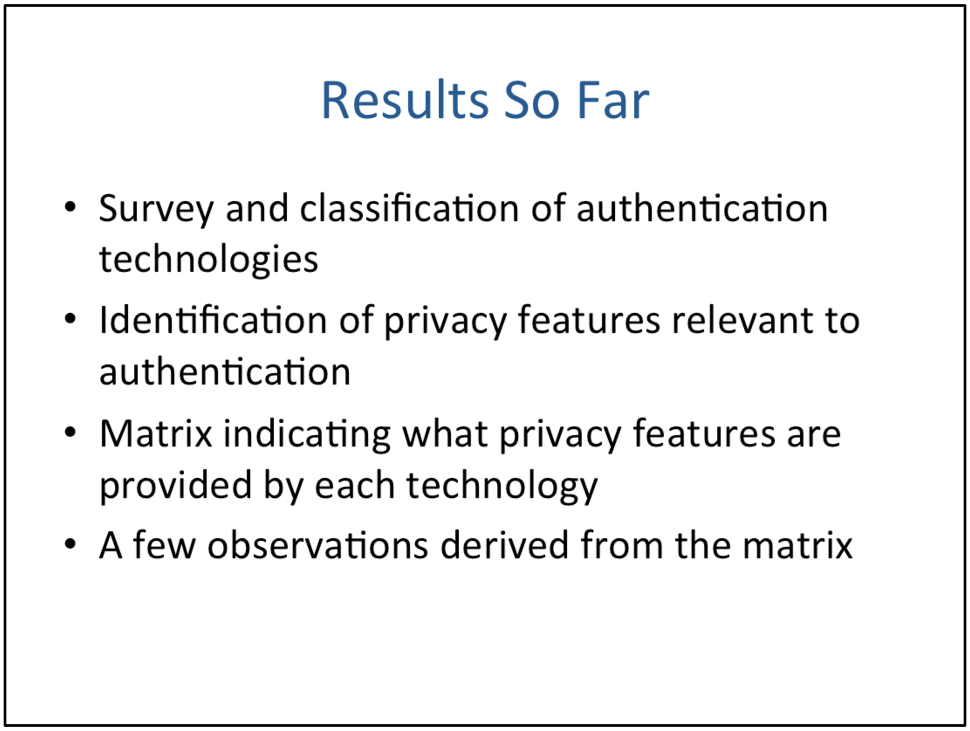
Goal

- Develop a conceptual framework for describing authentication technologies in terms that are both accurate and comprehensible to non-specialists
- First step: provide an actionable understanding of the privacy implications of authentication technologies

pomcor
pomcor.com

To address this obstacle, we want to develop a conceptual framework for describing authentication technologies in terms that are both accurate and comprehensible to non-specialists,

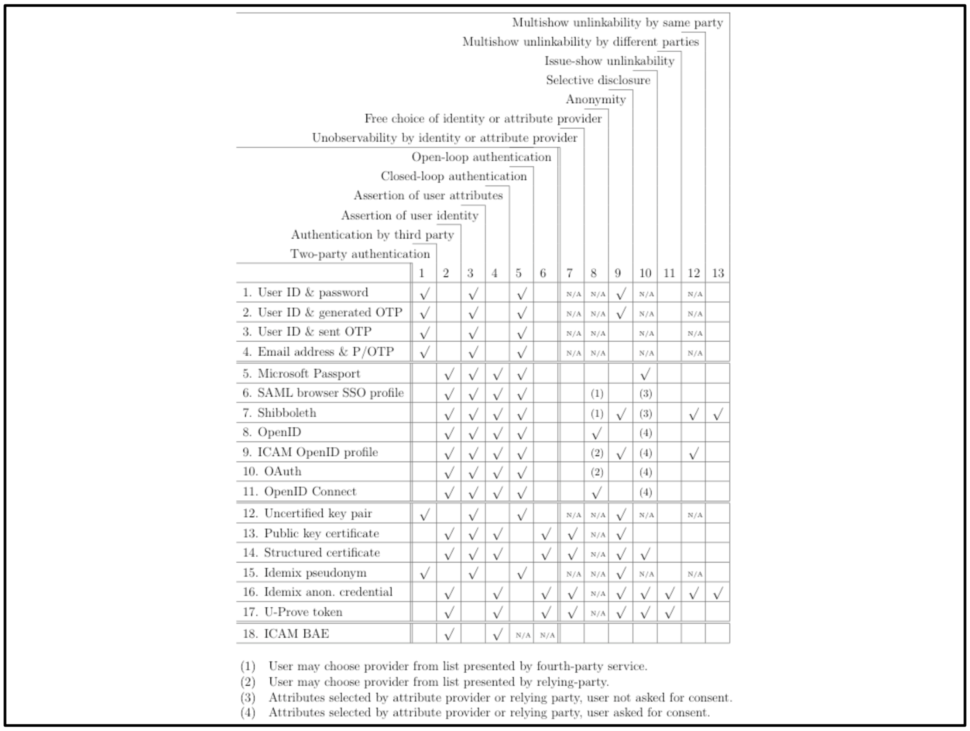
and as a first step, a framework that provides an actionable understanding of the privacy implications of authentication technologies.



Results So Far

- Survey and classification of authentication technologies
- Identification of privacy features relevant to authentication
- Matrix indicating what privacy features are provided by each technology
- A few observations derived from the matrix

Here are the results that we have achieved so far.
We have done a survey of authentication technologies and we have classified them along several dimensions, or facets.
We have identified a set of privacy features relevant to authentication.
We have built a privacy matrix indicating what privacy features are provided by each technology.
And we have derived a few observations from the matrix.



	Two-party authentication	Authentication by third party	Assertion of user identity	Assertion of user attributes	Closed-loop authentication	Open-loop authentication	Unobservability by identity or attribute provider	Free choice of identity or attribute provider	Anonymity	Selective disclosure	Issue-show unlinkability	Multishow unlinkability by different parties	Multishow unlinkability by same party
	1	2	3	4	5	6	7	8	9	10	11	12	13
1. User ID & password	√		√		√		N/A	N/A	√	N/A		N/A	
2. User ID & generated OTP	√		√		√		N/A	N/A	√	N/A		N/A	
3. User ID & sent OTP	√		√		√		N/A	N/A		N/A		N/A	
4. Email address & P/OTP	√		√		√		N/A	N/A		N/A		N/A	
5. Microsoft Passport		√	√	√	√					√			
6. SAML browser SSO profile		√	√	√	√			(1)		(3)			
7. Shibboleth		√	√	√	√			(1)	√	(3)		√	√
8. OpenID		√	√	√	√			√		(4)			
9. ICAM OpenID profile		√	√	√	√			(2)	√	(4)		√	
10. OAuth		√	√	√	√			(2)		(4)			
11. OpenID Connect		√	√	√	√			√		(4)			
12. Uncertified key pair	√		√		√		N/A	N/A	√	N/A		N/A	
13. Public key certificate		√	√	√		√	√	N/A	√				
14. Structured certificate		√	√	√		√	√	N/A	√	√			
15. Idemix pseudonym	√		√		√		N/A	N/A	√	N/A		N/A	
16. Idemix anon. credential		√		√		√	√	N/A	√	√	√	√	√
17. U-Prove token		√		√		√	√	N/A	√	√	√		
18. ICAM BAE		√		√	N/A	N/A							

(1) User may choose provider from list presented by fourth-party service.
(2) User may choose provider from list presented by relying-party.
(3) Attributes selected by attribute provider or relying party, user not asked for consent.
(4) Attributes selected by attribute provider or relying party, user asked for consent.

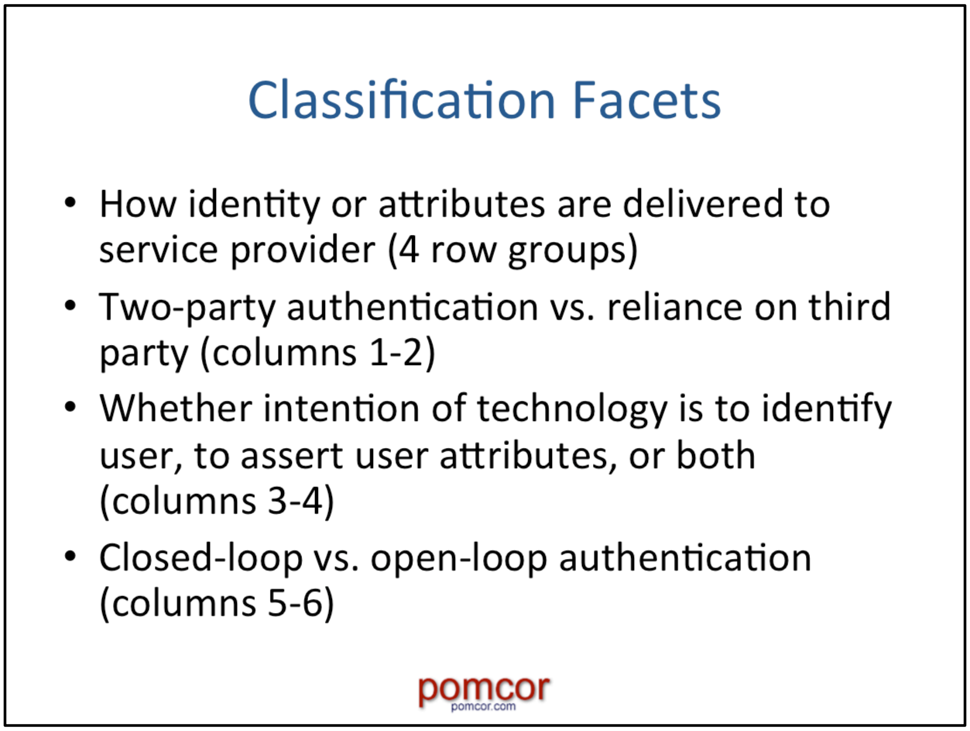
Here is a table that summarizes the classification and the matrix. It's in the paper and in the poster.

There are 18 rows corresponding to technologies or variants of technologies.

The rows are divided into 4 groups, which comprise one classification facet,

There are 3 pairs of columns on the left corresponding to 3 other facets,

and 7 columns on the right corresponding to 7 privacy features and indicating what technologies provide each feature.

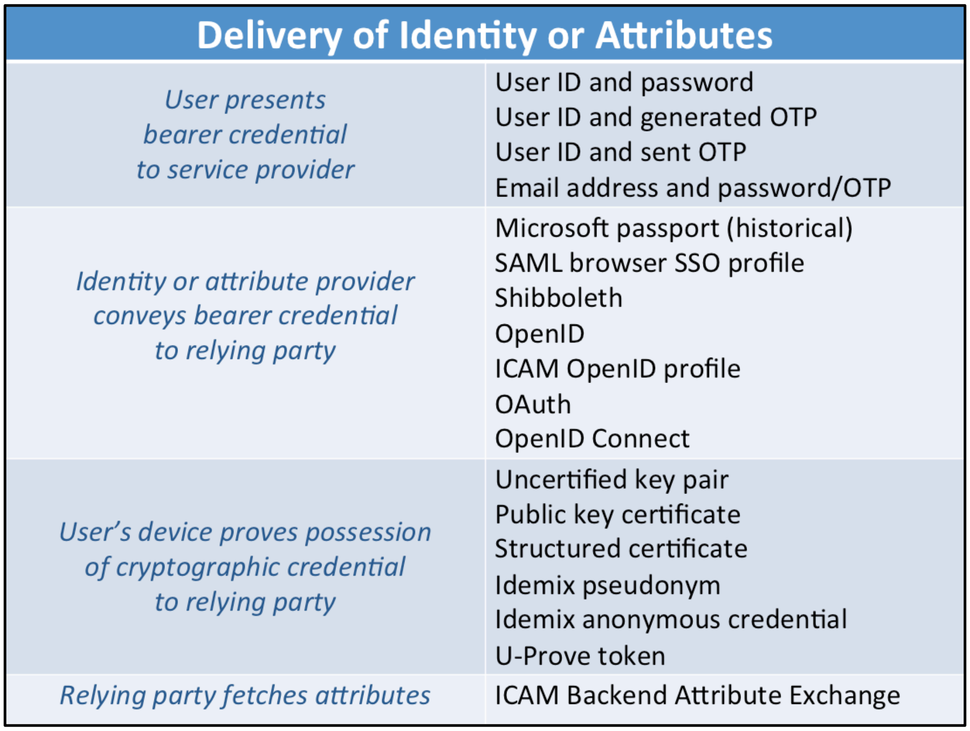


Classification Facets

- How identity or attributes are delivered to service provider (4 row groups)
- Two-party authentication vs. reliance on third party (columns 1-2)
- Whether intention of technology is to identify user, to assert user attributes, or both (columns 3-4)
- Closed-loop vs. open-loop authentication (columns 5-6)

pomcor
pomcor.com

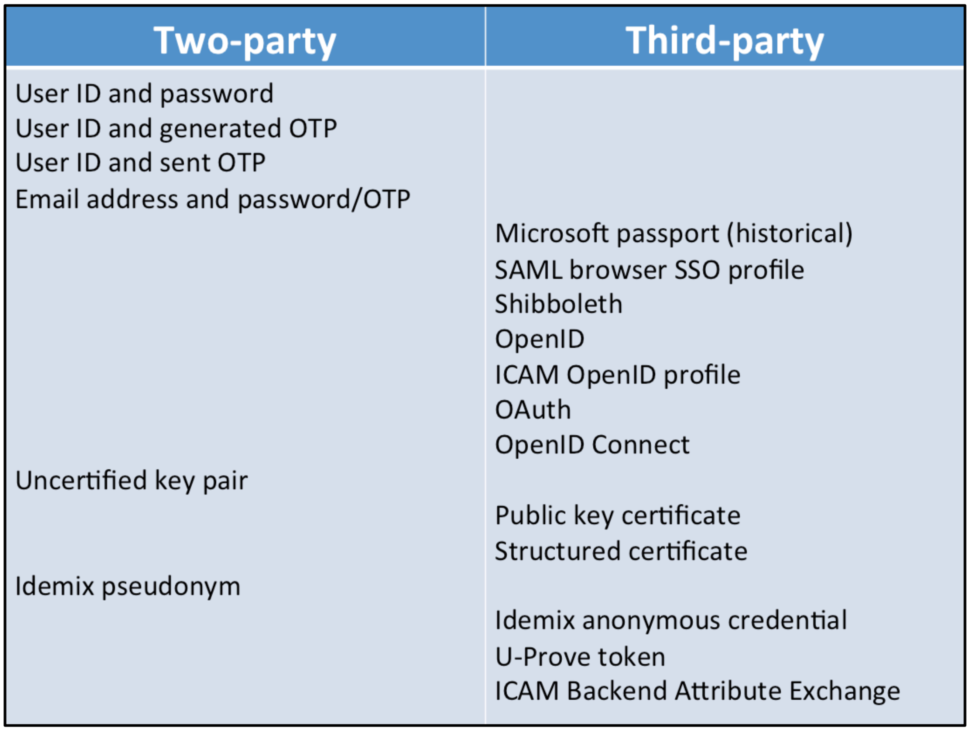
The classification facets are:
how identity or attributes are delivered to service provider.
two-party authentication vs. reliance on third party.
whether intention of technology is to identify user, to assert user attributes, or both, and closed-loop vs. open-loop authentication.
(The service provider, by the way, is the party that needs to know the user' s identity or attributes in order to provide some service such as access to an account.)
(The service provider is also called the relying party when there are more than two parties.)



Delivery of Identity or Attributes

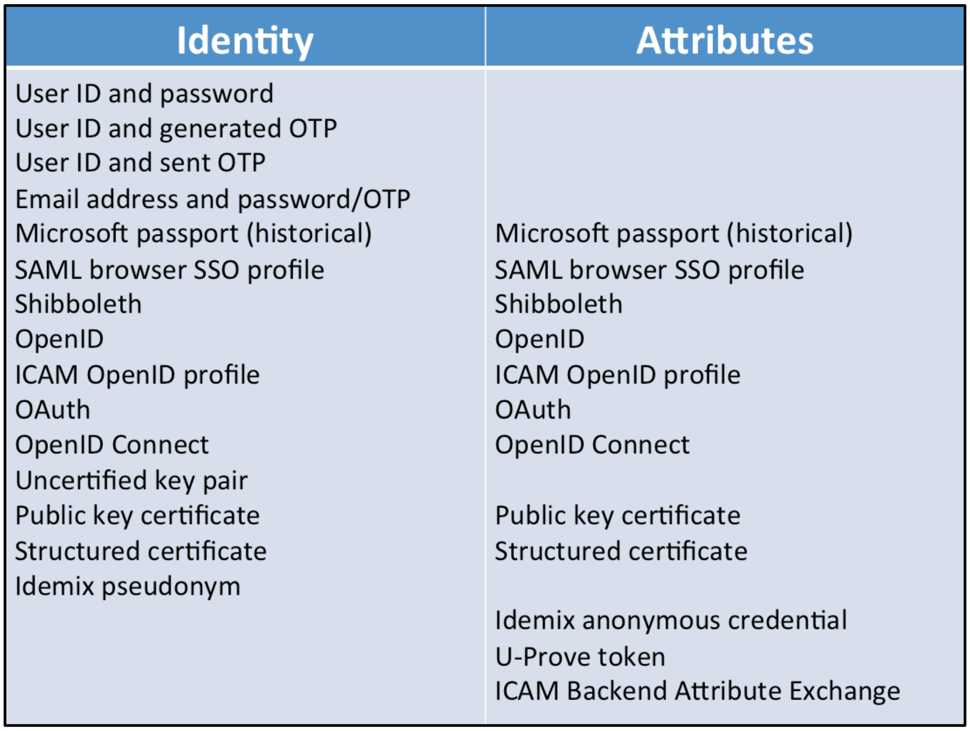
User presents bearer credential to service provider	User ID and password User ID and generated OTP User ID and sent OTP Email address and password/OTP
Identity or attribute provider conveys bearer credential to relying party	Microsoft passport (historical) SAML browser SSO profile Shibboleth OpenID ICAM OpenID profile OAuth OpenID Connect
User's device proves possession of cryptographic credential to relying party	Uncertified key pair Public key certificate Structured certificate Idemix pseudonym Idemix anonymous credential U-Prove token
Relying party fetches attributes	ICAM Backend Attribute Exchange

This is the first facet.
It is useful because it groups the technologies by technical similarity.
In the first group, the user presents a bearer credential to the service provider – this group includes passwords and one-time passwords.
In the second group an identity or attribute provider conveys a bearer credential with the user's identity or attributes to a relying party – this group includes Shibboleth, OpenID, Oauth, etc.
In the third group, the user's device proves possession of a cryptographic credential that asserts the identity or attributes to the relying party
And the fourth group contains a single technology, ICAM's Backend Attribute Exchange, which allows the service provider to fetch additional attributes from an attribute provider after authenticating the user.



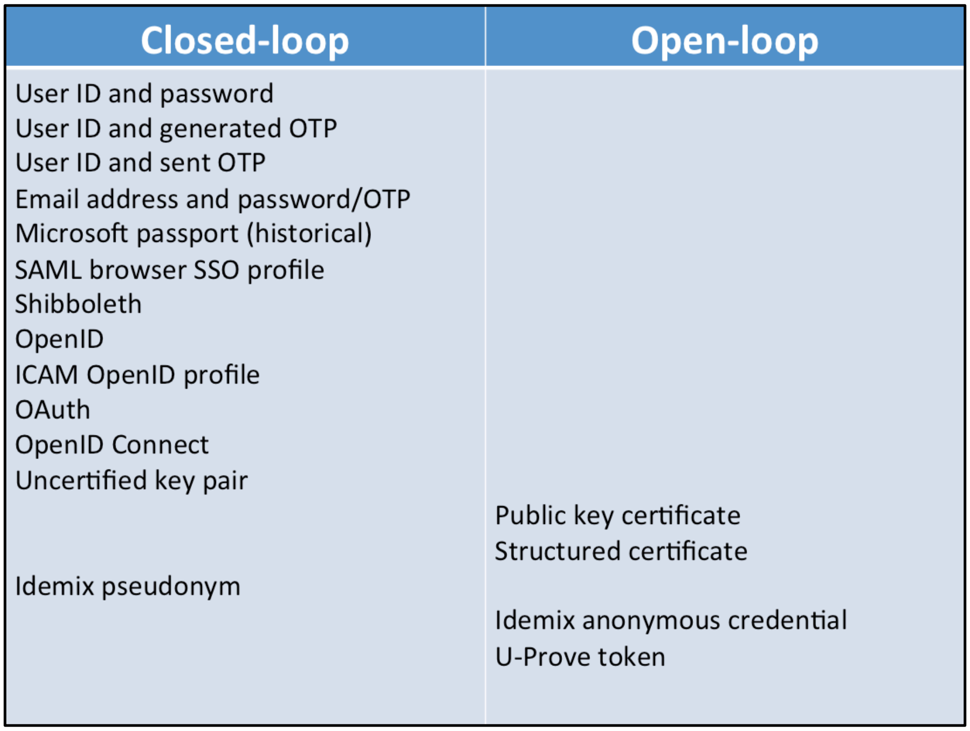
Two-party	Third-party
User ID and password	
User ID and generated OTP	
User ID and sent OTP	
Email address and password/OTP	
	Microsoft passport (historical)
	SAML browser SSO profile
	Shibboleth
	OpenID
	ICAM OpenID profile
	OAuth
	OpenID Connect
Uncertified key pair	
	Public key certificate
	Structured certificate
Idemix pseudonym	
	Idemix anonymous credential
	U-Prove token
	ICAM Backend Attribute Exchange

This is the second facet, two-party vs. third-party.
Two-party authentication technologies include passwords, one-time passwords, uncertified key pairs, and Idemix pseudonyms.
All the technologies in the left column involve an identity or attribute provider as a third party.



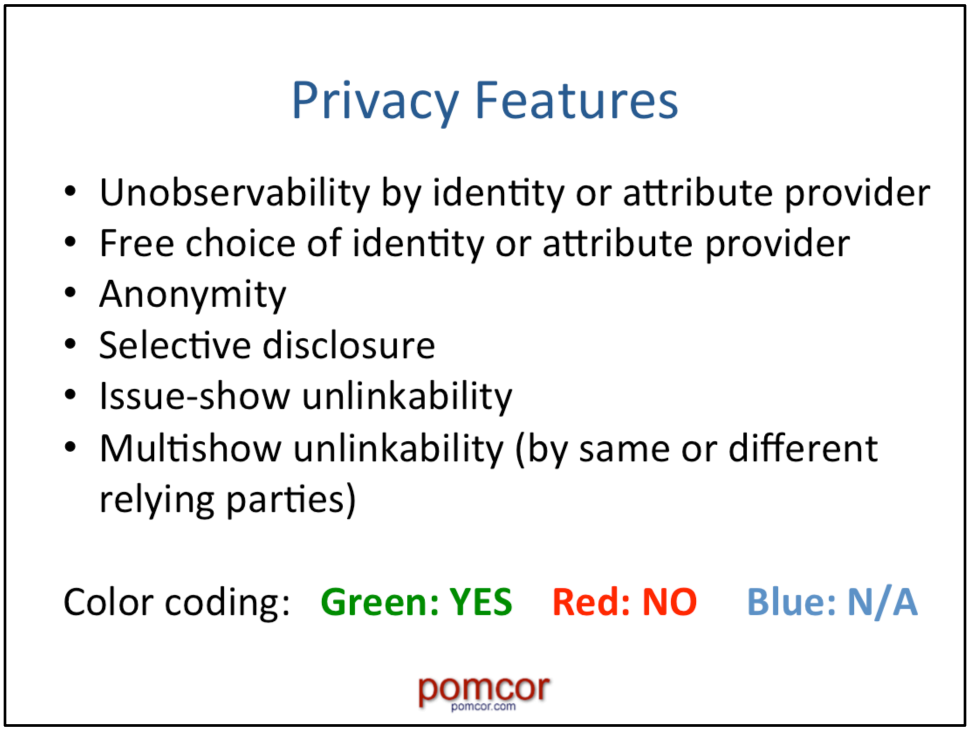
Identity	Attributes
User ID and password	
User ID and generated OTP	
User ID and sent OTP	
Email address and password/OTP	
Microsoft passport (historical)	Microsoft passport (historical)
SAML browser SSO profile	SAML browser SSO profile
Shibboleth	Shibboleth
OpenID	OpenID
ICAM OpenID profile	ICAM OpenID profile
OAuth	OAuth
OpenID Connect	OpenID Connect
Uncertified key pair	
Public key certificate	Public key certificate
Structured certificate	Structured certificate
Idemix pseudonym	
	Idemix anonymous credential
	U-Prove token
	ICAM Backend Attribute Exchange

This is the third facet, identity vs. attributes.
It'is a matter of intent.
Some technologies are intended to identify the user, some to provide attributes, and some to do either.



Closed-loop	Open-loop
User ID and password	
User ID and generated OTP	
User ID and sent OTP	
Email address and password/OTP	
Microsoft passport (historical)	
SAML browser SSO profile	
Shibboleth	
OpenID	
ICAM OpenID profile	
OAuth	
OpenID Connect	
Uncertified key pair	
	Public key certificate
	Structured certificate
Idemix pseudonym	
	Idemix anonymous credential
	U-Prove token

And this is the fourth facet, closed-loop vs. open-loop authentication.
This is a new facet that we've found very useful.
Closed-loop means that the same party that issues or registers a credential is later responsible for verifying possession of the credential at authentication time.
Open-loop means that an identity or attribute provider issues a credential and then is out of the loop at authentication time.
Two-party authentication is always closed-loop.
Cryptographic authentication with a certificate, an Idemix anonymous credential or a U-Prove token is open-loop.
Other third-party technologies, such as Shibboleth, OpenID, Oauth, etc., are closed-loop.



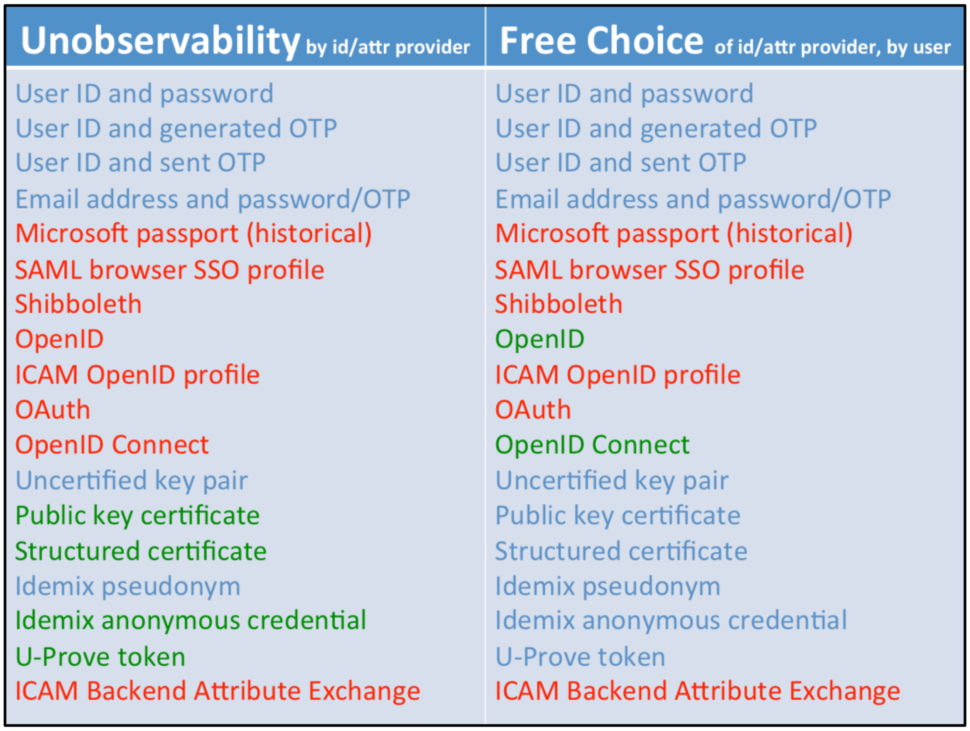
Privacy Features

- Unobservability by identity or attribute provider
- Free choice of identity or attribute provider
- Anonymity
- Selective disclosure
- Issue-show unlinkability
- Multishow unlinkability (by same or different relying parties)

Color coding: **Green: YES** **Red: NO** **Blue: N/A**

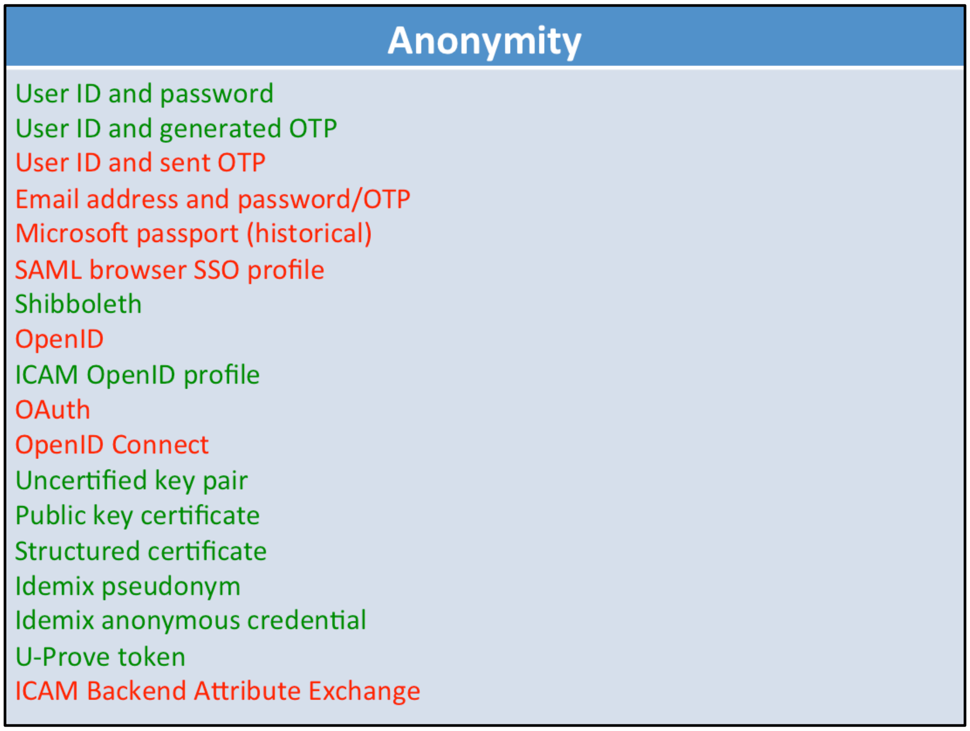
pomcor
pomcor.com

Here are the privacy features relevant to authentication:
Unobservability by the identity or attribute provider,
Free choice of identity or attribute provider,
Anonymity,
Selective disclosure,
Issue-show unlinkability,
And multishow unlinkability, which comes in several flavors.



Unobservability by id/attr provider	Free Choice of id/attr provider, by user
User ID and password	User ID and password
User ID and generated OTP	User ID and generated OTP
User ID and sent OTP	User ID and sent OTP
Email address and password/OTP	Email address and password/OTP
Microsoft passport (historical)	Microsoft passport (historical)
SAML browser SSO profile	SAML browser SSO profile
Shibboleth	Shibboleth
OpenID	OpenID
ICAM OpenID profile	ICAM OpenID profile
OAuth	OAuth
OpenID Connect	OpenID Connect
Uncertified key pair	Uncertified key pair
Public key certificate	Public key certificate
Structured certificate	Structured certificate
Idemix pseudonym	Idemix pseudonym
Idemix anonymous credential	Idemix anonymous credential
U-Prove token	U-Prove token
ICAM Backend Attribute Exchange	ICAM Backend Attribute Exchange

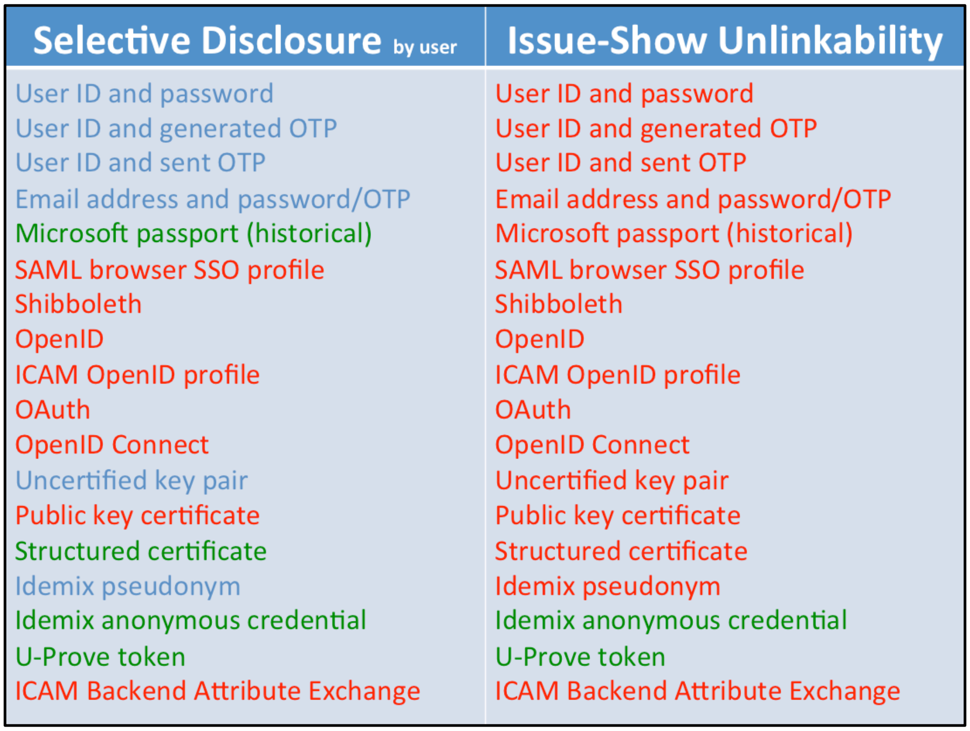
Here are the first two features.
Blue means that the feature is not applicable, green that it is provided, red that it is not provided.
Unobservability means that the third-party identity or attribute provider, when there is one, is not informed of the authentication event.
Open-loop authentication provides unobservability, but closed-loop authentication does not, because the identity or attribute provider is involved in the authentication event.
If there is no unobservability, it is desirable to let the user choose a trusted provider, but only OpenID and OpenIDConnect provide free choice.
OpenID Connect is an extension of Oauth with features found in OpenID, including free choice of identity provider.



Anonymity

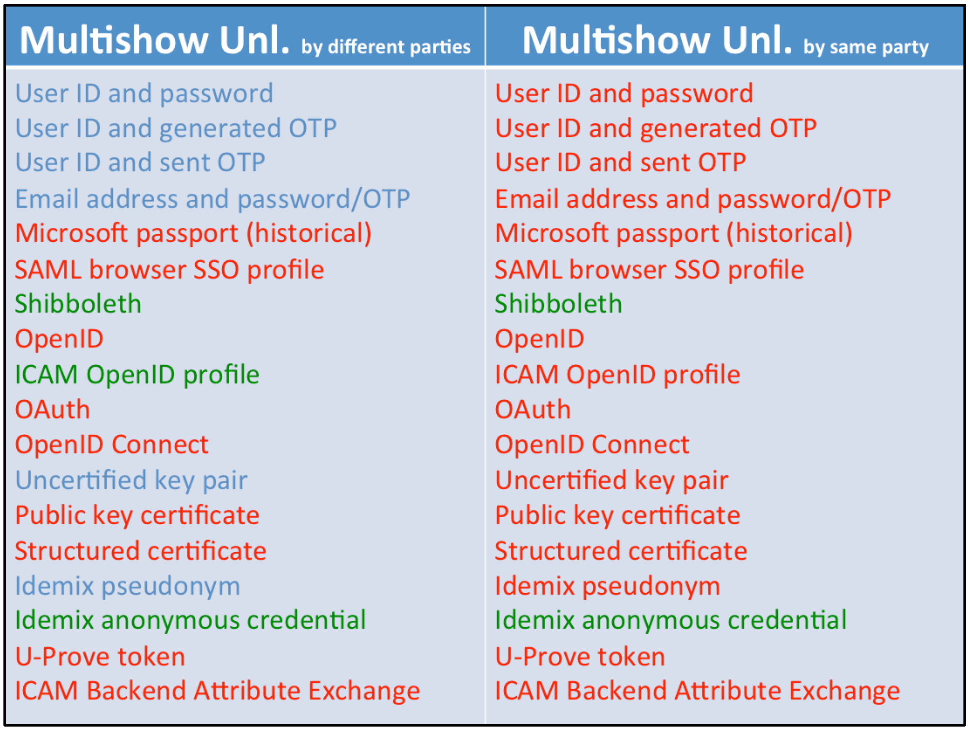
User ID and password
User ID and generated OTP
User ID and sent OTP
Email address and password/OTP
Microsoft passport (historical)
SAML browser SSO profile
Shibboleth
OpenID
ICAM OpenID profile
OAuth
OpenID Connect
Uncertified key pair
Public key certificate
Structured certificate
Idemix pseudonym
Idemix anonymous credential
U-Prove token
ICAM Backend Attribute Exchange

Anoher feature is anonymity.
An ordinary password provides anonymity if used in conjunction with a user ID freely chosen by the user, as opposed to an email address.
Open-loop authentication provides anonymity if used to assert attributes that do not uniquely identify the user.
Closed-loop authentication is typically intended to identify the user, but Shibboleth and the ICAM profile of OpenID provide anonymity.



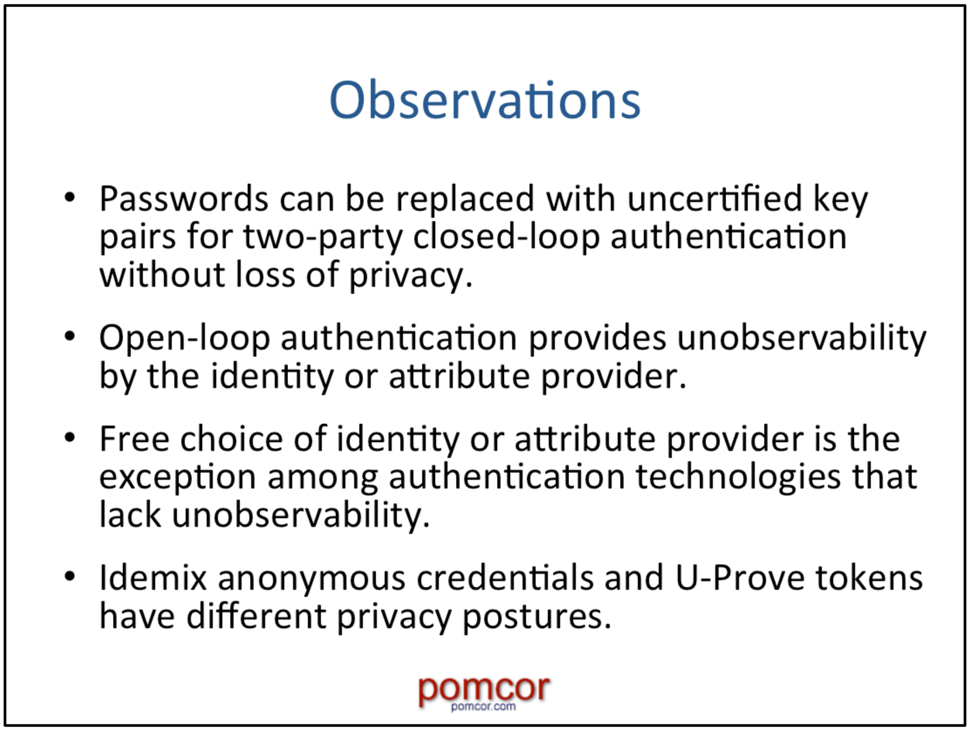
Selective Disclosure by user	Issue-Show Unlinkability
User ID and password	User ID and password
User ID and generated OTP	User ID and generated OTP
User ID and sent OTP	User ID and sent OTP
Email address and password/OTP	Email address and password/OTP
Microsoft passport (historical)	Microsoft passport (historical)
SAML browser SSO profile	SAML browser SSO profile
Shibboleth	Shibboleth
OpenID	OpenID
ICAM OpenID profile	ICAM OpenID profile
OAuth	OAuth
OpenID Connect	OpenID Connect
Uncertified key pair	Uncertified key pair
Public key certificate	Public key certificate
Structured certificate	Structured certificate
Idemix pseudonym	Idemix pseudonym
Idemix anonymous credential	Idemix anonymous credential
U-Prove token	U-Prove token
ICAM Backend Attribute Exchange	ICAM Backend Attribute Exchange

Here we get into the fancy privacy features that U-Prove and Idemix are famous for.
Selective disclosure means that the user can choose to disclose only partial information from a credential at authentication time.
Both U-Prove and Idemix are able to prove possession of a credential that has certain attributes without disclosing other attributes.
Idemix is also able to prove that a numeric attribute is greater than or less than a constant without revealing the attribute.
For example, it is able to prove that the user is old enough to buy wine based on a birthdate attribute without disclosing the birthdate.
Issue-show unlinkability means that it is not possible to tell whether a credential used in an authentication event is the same credential that was issued in a particular issuance event,
even if the credential issuer and the relying party collude.
Both U-Prove and Idemix provide this feature.



Multishow Unl. by different parties	Multishow Unl. by same party
User ID and password	User ID and password
User ID and generated OTP	User ID and generated OTP
User ID and sent OTP	User ID and sent OTP
Email address and password/OTP	Email address and password/OTP
Microsoft passport (historical)	Microsoft passport (historical)
SAML browser SSO profile	SAML browser SSO profile
Shibboleth	Shibboleth
OpenID	OpenID
ICAM OpenID profile	ICAM OpenID profile
OAuth	OAuth
OpenID Connect	OpenID Connect
Uncertified key pair	Uncertified key pair
Public key certificate	Public key certificate
Structured certificate	Structured certificate
Idemix pseudonym	Idemix pseudonym
Idemix anonymous credential	Idemix anonymous credential
U-Prove token	U-Prove token
ICAM Backend Attribute Exchange	ICAM Backend Attribute Exchange

Multishow unlinkability means that it is not possible to tell whether the same credential was used in two different occasions.
There are several flavors.
The ICAM profile of OpenID provides multishow unlinkability by DIFFERENT relying parties.
Closed-loop authentication technologies that do not necessarily identify the user, such as Shibboleth, can provide unlinkability by DIFFERENT parties and by THE SAME party.
Idemix anonymous credentials go a step further and provide multishow unlinkability by different parties and by the same party EVEN IF the credential issuer colludes with the relying parties.
A U-Prove token, on the other hand, does not provide multishow unlinkability.



Observations

- Passwords can be replaced with uncertified key pairs for two-party closed-loop authentication without loss of privacy.
- Open-loop authentication provides unobservability by the identity or attribute provider.
- Free choice of identity or attribute provider is the exception among authentication technologies that lack unobservability.
- Idemix anonymous credentials and U-Prove tokens have different privacy postures.

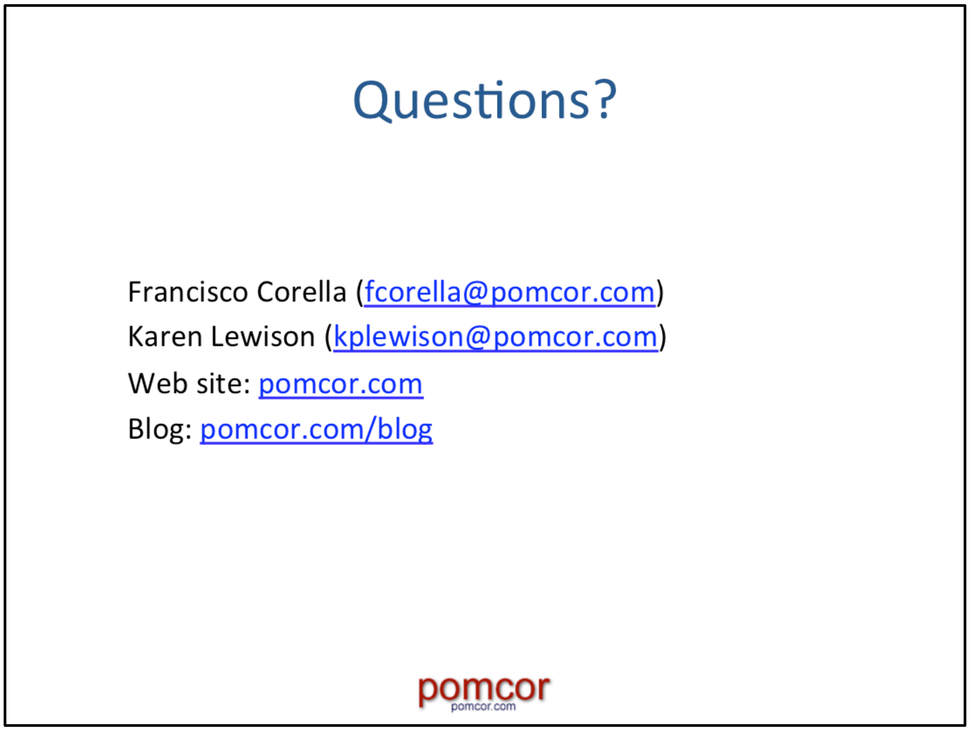
pomcor
pomcor.com

And finally, here are a few observation that can be made by looking at the matrix. Uncertified key pairs have the same privacy posture as ordinary passords, and can therefore achieve greater security than passwords without loss of privacy.

Open-loop authentication provides unobservability by the identity or attribute provider.

Free choice of identity or attribute provider is (unfortunately) the exception among authentication technologies that lack unobservability.

And Idemix anonymous credentials and U-Prove tokens have substantially different privacy postures.



Questions?

Francisco Corella (fcorella@pomcor.com)
Karen Lewison (kplewison@pomcor.com)
Web site: pomcor.com
Blog: pomcor.com/blog

pomcor
pomcor.com

See poster.