Privacy Postures of Authentication Technologies — ID360 Conference, April 30, 2013
Francisco Corella (fcorella@pomcor.com) and Karen P. Lewison (kplewison@pomcor.com)
Paper: pomcor.com/techreports/PrivacyPostures.pdf, site: pomcor.com, blog: pomcor.com/blog

Multishow unlinkability by same party													
Multishow unlinkability by different parties													
Issue-show unlinkability													
Selective disclosure													
Anonymity													
Free choice of identity or attribute provider													
Unobservability by identity or attribute provider													
Open-loop authentication													
Closed-loop authentication													
Assertion of user attributes													
Assertion of user identity													
Authentication by third party													
Two-party authentica	П		0		_		_			10		10	10
1 II. ID 0 1	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 3. User ID & sent OTP	\ \ /		\ \ /		\ \ /		N/A	N/A	V	N/A		N/A	
	\ \ /		\ \ /		\ \ /		N/A	N/A		N/A		N/A	
4. Email address & P/OTP	V		\ \ \ /	/	\ \ \ /		N/A	N/A		N/A		N/A	
5. Microsoft Passport		\ \ /	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	√ /			(4)		√ (2)			
6. SAML browser SSO profile		\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	√ /			(1)	/	(3)		,	/
7. Shibboleth		\ \ /	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	\(√ /			(1)		(3)		$\sqrt{}$	V
8. OpenID		\ \ /	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	√ /			√ (2)	/	(4)		,	
9. ICAM OpenID profile		$\sqrt{}$	$\sqrt{}$	\	\ \ /			(2)		(4)		$\sqrt{}$	
10. OAuth		\ \ /	\ \ /	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	\ \ /			(2)		(4)			
11. OpenID Connect	 ,	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	V	V					(4)			
12. Uncertified key pair	$\sqrt{}$,	$\sqrt{}$,	V	,	N/A	N/A	$\sqrt{}$	N/A		N/A	
13. Public key certificate						$\sqrt{}$	$\sqrt{}$	N/A	V				
14. Structured certificate						$\sqrt{}$		N/A	V	$\sqrt{}$			
15. Idemix pseudonym	$\sqrt{}$,			$\sqrt{}$,	N/A	N/A		N/A		N/A	
16. Idemix anon. credential		$\sqrt{}$				$\sqrt{}$	$\sqrt{}$	N/A		$\sqrt{}$	V		$\sqrt{}$
17. U-Prove token						$\sqrt{}$		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.

