PKI vs. non-PKI models

When Trust Frameworks for identity federations in different domains are compared, the inevitable question arises how policies of PKIs based on long-term credentials map to those that rely primarily on short-term assertions. To describe the two models the following table compares both approaches.

Model properties

Both models provide Identity Federation, policy mapping and multi-level security in the sense of Authentication Assurance Levels.

	PKI	*Non-PKI*
Technology		
• Client authN mechanism	X.509	X.509 and many others brokered by IdP
• Assertion type	Public key with long-term certificate	Short-term assertion from trusted party
• Protocols	X.509-based key validation	SAML, OpenID, WS-Trust, etc. X.509 to some extent
Federation use cases		
• End-to-end document security (sig, enc)	Yes	No (limited with services, PAKE etc.)
• Secure Channel with cryptographical binding	Yes (TLS)	Yes, with SAML HoK Profile
• SSO	Limited	Yes
• System to System comm.	Yes (Holder of Key)	Yes (HoK, Sender Vouches)
• AuthN with brokered trust[1]	No	Yes
• Pseudonymous IDs	No	Yes
• Attribute Provision	Very limited because of privacy and manageability	Yes, incl. RP-specific and user managed policies
• Mutual authN	Yes	Yes (using PKI)
• (Delegated) authZ	No	RBAC, ABAC, PBAC, OAuth
• Interfederation	Limited (constrained by Bridge-CA complexity)	Yes (Limits?)
• Code signing	Yes	No
• Mobile device 2FT AuthN[2]	Limited	OTP
Enterprise use cases		
• VPN client authN	Yes	No
• Physical Access Control	Yes	No

[1] Brokered trust: Subject authenticates with IdP, IdP provides assertion to RP

[2] Two factor token authentication

There might be some relevant use cases missing, but this comparison shows the advantages and application areas of each approach:

PKI is advantageous when a strong authentication to a system, network or service is required. Non-PKI-Systems offer more functionality and flexibility with use cases centered on HTTP, but depend on PKI for cryptographic client authentication at LoA 3+.

Positioning PKI and non-PKI

Federated IDM needs to use both PKI and non-PKI models to serve a broad range of use cases. Both models have their advantages and issues, and I would like to pick out a few where it is sensible to have options:

1. Authentication for web applications
   Non-PKI has the advantage, that IdPs can assure attributes and authorization policies in a flexible way. X.509-type authentication relies on backchannel queries to fetch that information. So in the PKI case the RP has to implement both an authN protocol and SAML attribute query or worse, depend on locally managed attributes and policies.
   In the non-PKI case it would be sufficient for the RP to implement SAML/OpenID/WS-Trust. SAML has the additional advantage that the RP might provide non-X.509 authN in the same package to other users for less stringent security requirements.
2. PKI security and usability issues
   PKI is hard in closed systems, but in open systems it is not realistic to rely on implementations for proper path validation, attribute processing, key usage, key management and certificate revocation. User interface in browsers is broken. Best practice is to rely only on X.509 core features and negotiate other properties outside this protocol.
   SAML Web-SSO and WS-Trust have their complexities, too, but given that these protocols serve two main purposes (Web-SSO and Web Services) the number of use cases and products is significantly smaller than with the ubiquitous X.509.
3. PKI and Bridge CA Certificate Policies as Trust Frameworks
   As CPs are geared towards to provision of credentials, influenced by RFC 3647, they tend to focus on the strength of the credential and leave other policy issues to the RP. Many are the RP's internal concern, but some are part of the trust relationship in the federation. A comprehensive Trust Framework needs to address all trust relationships.

Conclusions

- PKI and non-PKI federation models need to be combined in most cases at AL 3+
- For Web applications authentication with IdPs is beneficial in the majority of use cases and less bulky to implement and deploy.
- SAML can augment PKI in a way to reduce the X.509 complexity.
- To implement a federation an RFC 3647-style policy is insufficient.
- The Higher Education sector favors brokered trust (like inCommon), e-Government (see various eGov deployment profiles) and Industry (like 4 Bridges) prefer the PKI approach. There is a combination of both approaches.