XML Digital Signature in Mobile Environments

BACKGROUND

Mobile devices are becoming more important in day to day life whether it is for personal or business use. Mobile phones, wireless PDAs, and specialized wireless devices are being used to read email, perform inventory, get GPS location, and many more applications. As applications are pushed to the mobile environments, there are a number of challenges that need to be addressed. Traditionally, the challenges of mobile devices dealt with issues like size, weight, power, and connectivity. This has not really changed, but is complicated by layering additional requirements like XML Digital Signature on top of an already challenging problem.

THE CHALLENGE

Digital signatures provide mobile devices with two main challenges: increased size of data package (transaction); and the need for additional processing. Increased size of the data package ties directly into network connectivity and bandwidth. As the size of data packages decreases the signature becomes a very large part of the overall package and requires more connectivity and time to transmit the data. Digitally signing or verifying digital signatures also places a significant burden on a mobile device. In both operations, the XML data must be normalized using a canonicalization transform and then cryptographically processed. Both of these operations are very computationally intensive and have the potential of injecting enough latency to make the end user experience unacceptable.

POSITIONS

There are several activities underway that are attempting to address issues in the mobile computing environment that have the potential to be impacted by XML Digital Signature in a positive or negative way. If these technologies do not or cannot work successfully with XML Digital Signature then there is a risk that either XML Digital Signature or the other activities themselves will not be adopted. W3C should evaluate mobile initiatives to determine with which activities XML Digital Signature should be harmonized. There are still other technologies that target XML efficiency which should be evaluated for inclusion in the XML Digital Signature specification. Then again maybe the specification as written may not be well suited for mobile environments and other alternatives should be explored.

HARMONIZATION

Two of the initiatives under the W3C are Efficient XML[1] and the W3C Mobile Web Initiative[2]. Efficient XML has been developed to address throughput and performance issues related to the concerns of limited bandwidth and processing power in mobile platforms. The Mobile Web Initiative is aimed at making web browsing more useful for mobile users. Initiatives like these and others may be worthy of harmonization with XML Digital Signature.

INCLUSION

There are also technologies that may be relevant in mobile environments that should be examined for inclusion in XML Digital Signature. Technologies that improve cryptographic related efficiencies, like Elliptic Curve Cryptography (ECC)[3], should be considered for inclusion in the specification.

EXPLORATION

XML Digital Signature may not be suited for all mobile applications. Canonicalization is very costly with regard to processing power and time. XML digital signatures add size to documents (and packets) and can more than double the size of certain transactions. If XML is to be used securely in these environments then maybe a different solution needs to be sought for these applications or maybe a new approach would be warranted in general.

CONCLUSION

Mobile devices are a part of everyday life and users expect to be able perform the same functions securely in mobile environments as they perform in tethered environments. Consideration of mobile environment requirements when updating the specifications is prudent and should further the acceptance and implementation of specifications like XML Digital Signature.

---

[1] W3C Efficient XML Interchange Working Group - http://www.w3.org/XML/EXI/
[2] W3C Mobile Web Initiative - http://www.w3.org/Mobile/
[3] The Case for Elliptic Curve Cryptography - http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm