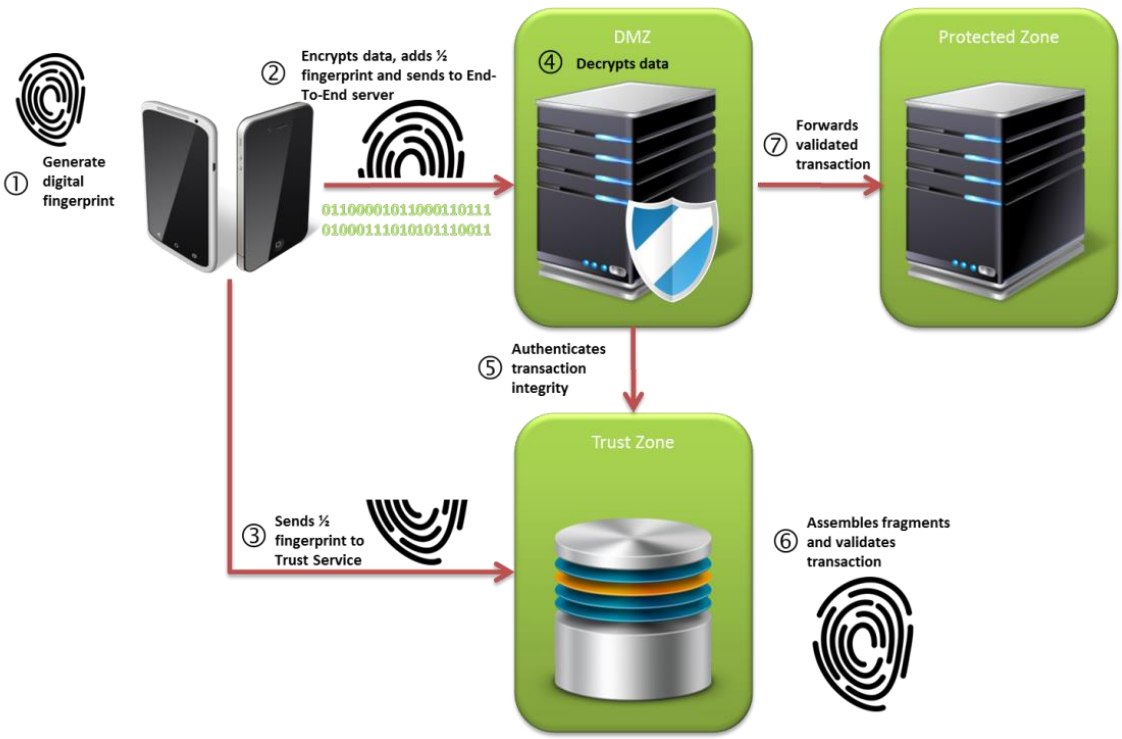
The m:Cypher® Network & Application Security platform underpins the m:Cypher® Payments solutions to provide the world's most secure online and mobile commerce environment.

m:Cypher® combines symmetric and asymmetric ciphers to deliver secure point-to-point encryption between client and server. Unable to be intercepted and observed via man-in-the-middle attacks, an m:Cypher® transaction also carries a digital fingerprint that certifies the authenticity of the transaction. This digital fingerprint, tightly derived from user & device identifiers and from the data payload, authenticates the source of the transaction and ensures that the data has not been tampered with during transmission between the client and server.



m:Cypher® uniquely splits the digital fingerprint and sends one fragment to the server and a second fragment to a Trust Service. The Trust Service assembles the fingerprint fragments, validates the integrity and provenance of the transaction, and returns an authentication code.

Network & Application Security

powered by mCYPHER®

Data security standards provide a framework to secure data centre and office IT environments. But what is happening outside of your control? Web sites and Web APIs provide anywhere, anytime access to internet banking and payment services but public networks and iOS/Android application store distribution hugely increase the surface area for attackers to discover and exploit weaknesses.

m:Cypher® Network & Application Security addresses fundamental weaknesses in HTTPS communications and helps secure payments within mobile applications .

Network Security	Data is encrypted inside SSL/TLS tunnel. Cannot be observed even if request is proxied
	Hides service end-point behind encryption firewall. Reduces attack surface
	Verifies transaction integrity. Transaction cannot be tampered with
	Unique Id to each request. Transaction cannot be replayed
	Out of bounds authentication user/device relationship. Authenticates transaction source
Application Security	PIN / Password entry to unlock encrypted data store. User has to authenticate with the application
	Application, Device & User affinity restricts access to server resources to authenticated users
	Policy driven lock, block and destroy rules for data store

AIB Merchant Services
6 Belfield Office Park, Beaver Row, Clonskeagh
Dublin 4, Ireland
01 218 2100 Ire.
0345 266 0591 UK
00353 1 218 2100 Int.
www.aibms.com

Actus Mobile Solutions
Atlas Court, IDA Business Park. Bray
Co. Wicklow, Ireland
01 902 3966 Ire.
0203 238 3992 UK
00353 1 902 3966 Int.
www.actusmobile.com