



Trust, Tokenization and Tokens

Rakesh Radhakrishnan
VP, Sr. IAM Architect
Enterprise Security Architecture

Bank of America DISCLAIMER

- None of the Contents in this presentation represent any REAL Bank Project. The material presented is Generic to Banking Industry and Standards bodies

The evolving definition of a “Tokenization”

- Tokens represent an Attribute Set (token types) -compressed or condensed - for example Perimeter host admission control solutions validate 60+ attributes about a device and then create a posture token (3 or 4 types - that reflects the Attribute sets)
- Tokens have some meta-data based on their characteristics (for example in the analogy above - green could mean healthy device, blue could mean device in quarantine, yellow could be unknown posture and red could mean defect in device)
- Tokens are Cryptic - meaning that if you are not briefed in advance - all the substance in the token will mean nothing to you (in our technology trend they are encrypted and compressed -secure exchange)
- Tokens represent Attributes with some level of Assurance -Attribute Assurance - since they are based on successful execution of some control function (validation of attributes and credentials)
- Tokens are generated at run time and have real time characteristics of a state of an Entity (entity can be subject or a resource or an action or condition) - real time representation of entities.

The evolving SCOPE of a “Security Token”

- Hard Tokens and Soft Tokens (Initiating Vector, Calculated Vectors, in a Vault)
 - Public Tokens vs. Private Tokens (between Enterprise within an Enterprise)
 - Standardized Tokens vs. non-Standardized Tokens (SAML vs. proprietary tokens)
 - Authentication Tokens vs. Access Tokens (RBAC token, XrML token, ACL token)
 - Subject Tokens vs. Resource Tokens (Human and Non-human representation)
 - Integrity Tokens vs. Trust Tokens (reputation, posture, TPM, SIM, etc)
 - Computed Token Types (many – application specific VDS technology)
 - Risk Tokens (for subjects and resources)
 - Transaction Token Types (such as SWIFT Tokens & IdenTrust Tokens)
 - Network Token Types (such as Posture tokens and Path tokens)
 - Decision Tokens and Obligatory Tokens
 - Data Tokenization (PCI-DSS, PII, etc., such as Protegrity)
-
- See <http://www.network-identity.com> (upcoming Book on “Identity & Trust for Controlled Cloud Computing” is all about Tokens and Trust (2014))

Tokens → pre and post CONTROLS

- Context driven Alignment (AuthN Context= Subject/entity and AC Context = Resource/Action)
- PCI-DSS, PII, iITAR and other Data Specific Control Alignments
- Streamlining Authentication = Type of AuthN = Token = Construct of Credentials
- Mimic Real World – Credential's (Assured Attribute Sets) equates to Access
- Streamline and Leverage Tokenization (Public STS, Private STS, Network STS, Risk & Data STS, etc)
- Integrate with Context Aware Security Systems (IAM with Net & Info Sec)
- Mitigation Strategies require Continuous Alignment of Integrated Controls
 - Preventive Controls
 - Concurrent Controls
 - Reactive Controls
 - Obligatory Controls
 - Mitigating Controls

Layer 1 -7 + 2 more (Identity & Policy)

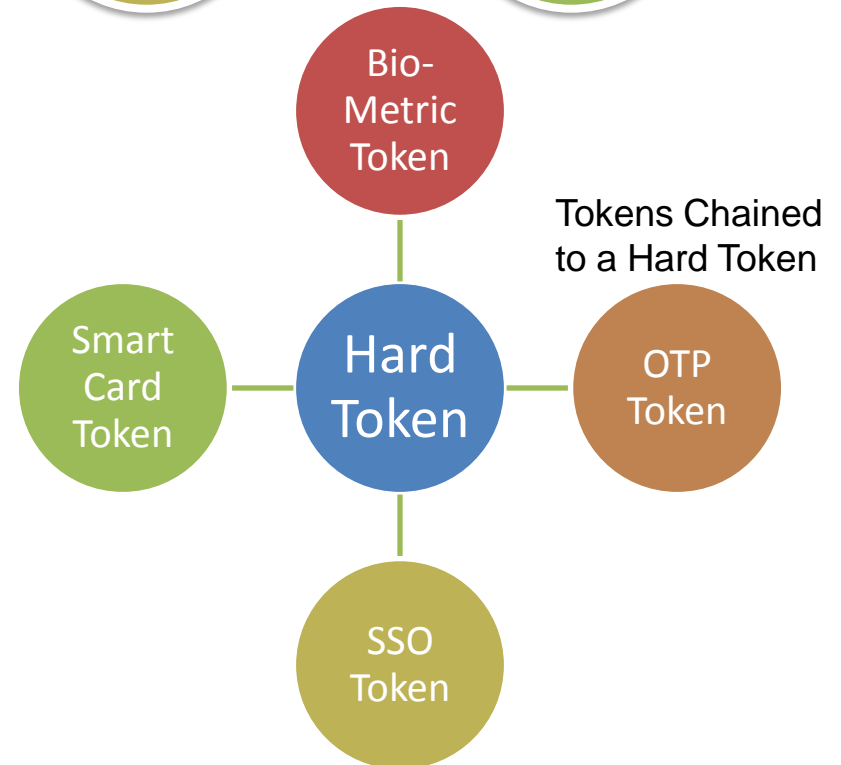
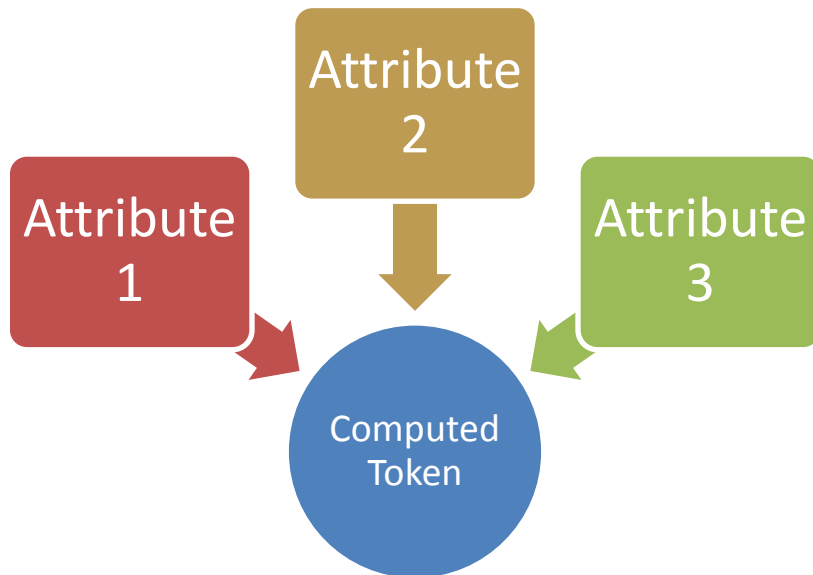
Layers	Example Tokens	Token Combination leads to specific Levels	Control Functions augmenting –RBAC, ABAC, T-BAC
USER	OTP Token, Bio-metric tokens, etc.	Subject IA/AA Levels	User & resource level Access Control
Application Layer	Kerberos Token, RDF token, etc.	Resource Trust Level	App Protocol Control
Presentation Layer	Data Tokens, USB Tokens, DOM token, etc.	Risk Levels and Integrity Levels	Coding & Conversion Controls
Session Layer	SSO Token, CDSSO token, Network Token	Integrity Level, Trust Level	Session Control
Transport Layer	IP/Host Identity Protocol /HIP token	Integrity Level, Trust Level	Flow, Port and Header Control
Network Layer	Packet Token, Posture Token, TNC token, Path Token, Periphery Token etc.	Integrity Level (subject and resource)	IP Address and Routing Control
Data Link Layer	MAC Address Token, PSS toke, TPM token, etc.	Trust Level Subject IA/AA Level	(physical) media access control

Assimilating Token Types for Alignment

Token Combinations Impacts Subject Assurance Levels



Computed Tokens from Attributes

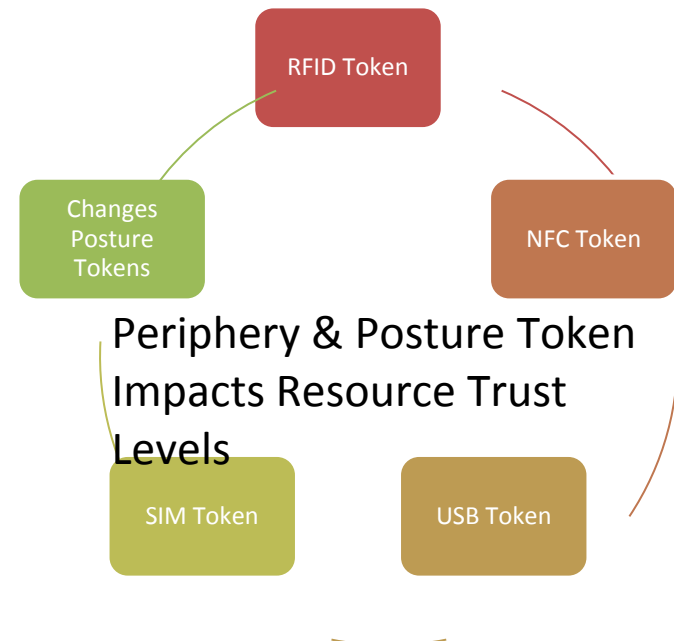
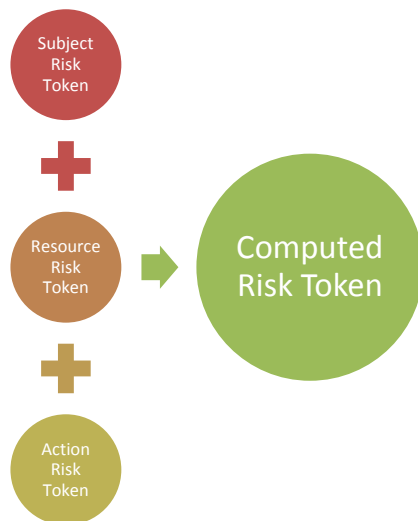


Assimilating Token Types for Alignment

Token Combinations Impacts Resource Trust Levels



Computed Composite Risk Token



Background Papers on Tokens

1) <http://www.utdallas.edu/~hamlen/khaled-cloudcom10.pdf>

This paper validates the fact that just like subject are represented as TOKEN's in today world – the challenges associated with representing distributed resources as Token's are attempted to be addressed by the Academic and Security Standards world – RDF/Semantics

2) <http://ipdps.cc.gatech.edu/1997/wocs/hapinkst.pdf>

This paper describes the Token based approach for a TDMA network – tokenizing the packets at the Data Link Layer –in conjunction with potential hard tokens – this is being expanded to all MPLS networks – multi-protocol label switching networks and 4G like high bandwidth network –where we can afford to add another token insertion between data packets and the header packets to validate INTEGRITY of PATHS Connections and more

3) http://csrc.nist.gov/news_events/privilege-management-workshop/PvM-Model-Survey-Aug26-2009.pdf

The above NIST paper – discusses RBAC 1st and then ABAC – it also sees a future in Policy BAC(PBAC) and the RiskAdaptiveAC (RadAC) The next stage beyond 2012 is to evolve Token BAC (that leverages the NG Tokenization Technologies to abstract RBAC, ABAC and RiskBAC)

4) http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/PstrVal.html#wp24141 A cisco paper on cisco security product lines that have started tokenization's (posture token for example acts as an input to the INTEGRITY Token and Integrity Level that we compute in T-BAC –token buckets are utilized by Cisco ASA to compute integrity tokens)

5) http://securosis.com/reports/Securosis_Understanding_DBEncryption.V.1.pdf SecureOSIS paper on Data Tokenization and Encryption

6) <http://accelconf.web.cern.ch/accelconf/ica07/PAPERS/TPPA04.PDF> A paper describing how RBAC profile can be expressed in XML as x-rbac and how the XML profile can be tokenized with a MAP

7) http://publib.boulder.ibm.com/infocenter/wsdoc400/v6r0/index.jsp?topic=/com.ibm.websphere.iseries.doc/info/ae/ae/cwbs_xmltoken.html A paper describing how Rights Management in a DRM or IRM system can be expressed in XML using XrML and any XML profile again can be tokenized XrML token

8) <http://download.oracle.com/docs/cd/E19253-01/816-4557/aparecord-3/index.html> A paper describing the expression of ACL (access control lists) as ACL token

9) http://www.ece.cmu.edu/~peha/network_PTB.pdf

<http://repository.cmu.edu/cgi/viewcontent.cgi?article=1046&context=epp&sei-redir=1#search=%22priority%20token%22>

Papers describing Permission Token (including white list black list) & Priority Token