



# Identity Safe Harbor

Virginia Joint Commission on Technology and Science

17 October, 2012

**CertiPath**

# Cyber Security Today



Without the identity  
problem solved ...  
we can only keep honest  
people honest.



# The Devolution of Identity: Anonymity Breeds Crime



- July 5, 1993
- Every day since



## Stolen Identity Dangers



## 7 Things ID Thieves Could Fund With Your Stolen Tax Refunds



## ICE holds Nigerian admitting to using false ID to work at airport



## Tax Refund Hung up Due to Stolen Identity

## U.S.: Identity theft grows as hackers get savvier



# Quick Recap of JCOTS Efforts



- September 21<sup>st</sup>, 2011
  - The initial presentation of an identity safe harbor bill was presented to JCOTS
- 4Q11-2Q12
  - Minor modifications to draft bill and socialization of need
- July 17<sup>th</sup>, 2012
  - JCOTS heard from John Biccum of Microsoft
    - Key Message - online identity was among the most important problems to be solved
  - Verizon and CertiPath provided concurring observations

# Why we Need Identity Safe Harbor



- In effect – with respect to liability - we don't know what we don't know
  - You will not win the hearts and minds of CFOs with this
  - We have 10 years of slow, random adoption as a result
- Bill makes the distribution of liability predictable
- It is mostly analogous to the distribution in the credit card model
  - Identities, like credit cards, are not used solely in one geo-politically defined area – identity legislation needs to be mindful of inter-state usage

If the incentives line up with the behavior you want, you get compliance. Ideally we reward good behavior.

# How Do we Measure Good Enough



- Trust Frameworks and Trust Framework Providers
  - Think Visa, Mastercard, AMEX, etc.
- The bill presently has Federation/Federation Operator
  - This is one possible way to go but is not the most flexible
- Recommendation:
  - Substitute Trust Framework for Federation
  - Benefit:
    - Virginia is able to pass policy that is essentially future proof while allowing operational control to react to the dynamic environment
      - E.g. – Virginia keeps a list of approved Trust Frameworks (and their providers) which the bill points to but doesn't incorporate by specific name

# You've Been Down this Road Before



- Remote Notary Law
  - Best possible illustration as it incorporate multiple concepts:
    - Substitution of token representing past identity establishment for a new person proofing
    - Token is constrained by the trust framework/federation it was issued under
      - Specifically the Federal Bridge for PIV/PIV-I
  - Shows a recognition on the behalf of the State of Virginia that
    - Security can be improved while reducing cost
      - Accepting PIV/PIV-I is stronger than what the notary process was before
      - Skips in person proofing at the beginning of notarization workflow
      - Citizen Impact: Enables more convenient notarization

# Fraud Reduction



- Identity centric citizen services is just the beginning
- Identity at the Federal Level was tied to 9/11
  - Authentication to resources is the main use case
- Identity at the State Level will be tied to Fraud Reduction
  - This is a more advanced use case
  - It's all about the Attributes
    - Which ones
    - How are they vetted
    - How often are they re-vetted/how are updates discovered and made
    - What do we call them
    - AND
      - How do we trust them from other states ... and vice versa

# The Present Environment in Virginia



- Reduction of Fraud is largely understood to be a self-funding problem to solve
  - Partially automating and streamlining the entitlement workflow will reduce cost significantly too
- No State has fully implemented a solution
  - ... But Virginia is further ahead in the right areas than anyone else
    - EDM is literally the best possible architecture a state could implement
    - CAS is a type of authentication gateway – again best-of-breed
- States, in general, have an additional challenge
  - Large scale of entities juxtaposed with a lack of centralized authority
  - Belong to a COI that is less centralized yet .. And by design

# Communities of Interest (COIs)



- Any group of disparate parties (typically smaller groups) with a need to interact.
  - Federal Agencies, Aerospace and Defense companies, institutions of higher learning and ... States
- States as a COI can be a bit daunting
  - Defined population
    - But its transient
  - Provides services
    - But often beyond its own population
- Members of a COI are often IdPs and Service Providers
  - Virginia must consider that it relies on its own resident identity data as well as that provided by other states

# Trust Framework



- Interstate Coordination
  - Required if we are to achieve policy, legal and technologically interoperable identity data sophisticated enough to reduce fraud
- Trust Frameworks and the Trust Framework Provider
  - The governance and C&A function that insures coordination within a COI
  - In the Federal and Aerospace and Defense COIs, the Federal Bridge and CertiPath have served this function for the past decade
- To date, TFs have sought to support core identity only
  - States require much more ... a new Trust Framework is required

# The State Bridge



- Minimum of 5 states will charter this Trust Framework
  - Virginia will be invited to join in recognition of their work to date and ability to make use of interoperable identity in the short term
  - Policy Management Authority membership requires “Skin in the Game”
- Initial decisions to be made at the PMA
  - Safe harbor and other legal considerations for state identity providers
  - Supported state credentialing model
    - Insource, Co-source, outsource (I.e., Public or Public/Private Partnerships)
- Looking for input from:
  - State applications which are concerned with fraud
    - Attributes requirements
  - Applications that interact with other states or other state residents
    - Interoperability requirements