



Connect Virginia

Advancing Virginia's Health Care

HITSAC Identity and Access Management Overview

July 19, 2012



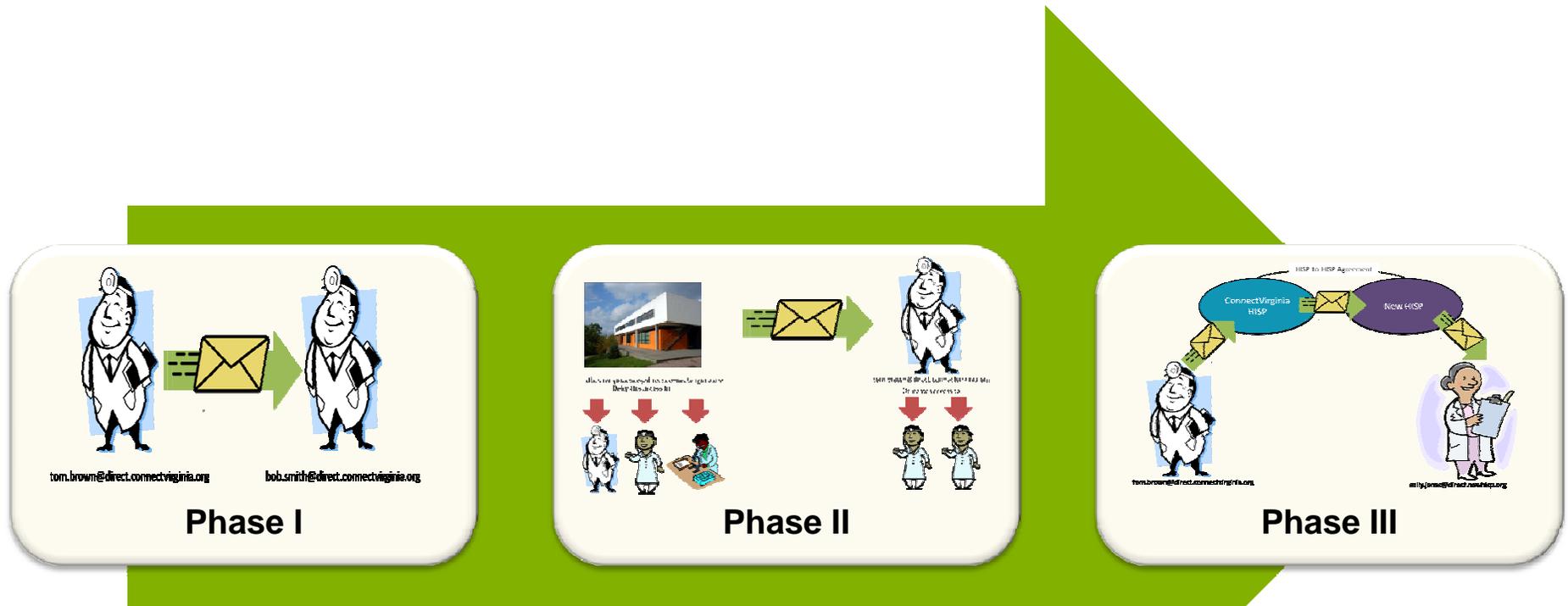
Agenda

- Overview of ConnectVirginia
- ConnectVirginia Identity Management & NIST
 - Why?
 - How?

Connect Virginia Overview

- Led by Community Health Alliance, Inc.
 - Sandy McCleaf – Executive Director
 - Michelle White – Program Manager
- Connect Virginia is the Statewide Health Information Exchange (HIE) for the Commonwealth of Virginia
 - Connect Virginia EXCHANGE
 - Connect Virginia DIRECT Messaging Service
- Visit www.connectvirginia.org for more information

ConnectVirginia Direct Messaging



Identity Management Overview

Why NIST (SP 800-63-1)

- Ensure alignment with Commonwealth of Virginia Identity Management standards (e.g. VITA, DMV)
- Establish confidence in user identities
- Adopt a standards based approach
- Compliance with NIST assurance Levels 1-3
- How???

Registration & Identity Proofing

NIST Guideline

1. *An Applicant must apply to a Registration Authority (RA) to become a Subscriber of a Credential Service Provider (CSP). In the registration process, an Applicant must undergo identity proofing by a trusted RA.*

ConnectVirginia

1. ConnectVirginia achieves Level 3 Assurance by:
 - a. Requires that all applicants complete an enrollment form to begin registration.
 - b. Requiring the applicant notarize the enrollment form prior to submission.
 - c. Verifying the status of the applicants professional medical license prior to approval
 - d. Periodically reviewing the status of the individuals professional license
 - e. Maintaining records of each individual who has been identity proofed
 - f. Adopting policies that require the Registration/ID proofing requirements above

Issuing Tokens & Authentication

NIST Guideline

1. A token contains a secret to be used in authentication processes.
2. A token can take many forms and may exist in hardware, software or human memory.
3. Tokens are possessed by a Claimant and controlled through one or more of the traditional authentication factors (*something you know, have, or are*)

ConnectVirginia

1. ConnectVirginia achieves a Level 3 assurance by requiring the following two types of authentication factors:
 - a. *Memorized Secret Token* - A secret shared between the Subscriber and ConnectVirginia and is considered **“something you know”**.
 - b. *Single-factor OTP Device* - A spontaneous generation of one-time passwords delivered to the subscribers mobile device via SMS message. Considered **“something you have”**

Technology Approach

SAML

1. Tightly Coupled
 - a. Configuration required
 - b. SSL key exchange typically required
 - c. Custom coding typically required
2. Low adoption in private sector
 - a. Custom effort to be able to login
3. Inconsistent Implementation
 - a. Example: Attributes vary
4. Determination of what is accessed is between systems

OAUTH

1. Loosely Coupled
 - a. Configuration of identifiers required
 - b. No SSL key exchange
 - c. No custom coding
2. Widely adopted in private sector
3. Consistent implementation
4. Determine of what is accessed could be approved by the user.

Connect Virginia Two-Factor Authentication



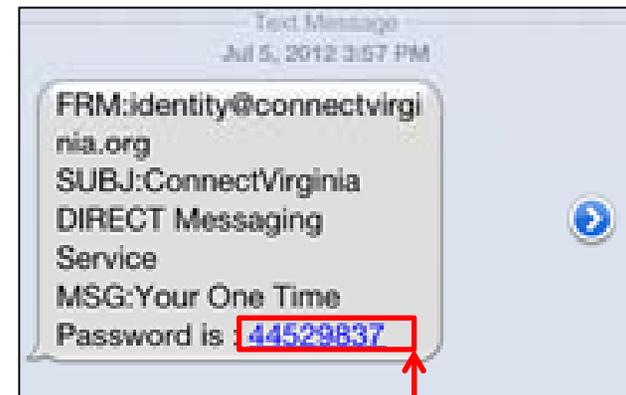
Connect Virginia
Advancing Virginia's Health Care

Sign in to Connect Virginia's DIRECT Messaging Service

User Name:

Password:

This service is powered by MEDfx. Copyright © 2011-2012 MEDfx. All rights reserved.



Text Message
Jul 5, 2012 3:57 PM

FRM:identity@connectvirginia.org
SUBJ:Connect Virginia DIRECT Messaging Service
MSG:Your One Time Password is : **44529837**

Memorized Secret Token: "Something You Know"

Single-factor OTP Device: "Something You Have"



Connect Virginia
Advancing Virginia's Health Care

Your One Time Password has been sent to your email or mobile device.
The password will expire in 03 minutes 05 seconds

Enter OTP Code:

This service is powered by MEDfx. Copyright © 2011-2012 MEDfx. All rights reserved.



Questions?