

DirectTrust

Collaborating to Build the Security and Trust
Framework for Direct Exchange

David C. Kibbe, MD MBA

David.Kibbe@DirectTrust.org

July 24, 2013

Mission and Goals



DirectTrust.org, Inc. (DirectTrust) is a voluntary, self-governing, non-profit alliance dedicated to the support of Direct exchange of health information at national scale, through the establishment of policies, interoperability requirements, and business practice requirements. Taken together, these create a Security and Trust Framework for the purpose of uniting multiple Direct implementations and their communities, enhancing public confidence in privacy, security, and trust in identity when using Direct.

DirectTrust is the recipient of an ONC Cooperative Agreement award in the amount of \$280,205 as part of the Exemplar HIE Governance Program. Within this Program, DirectTrust is charged by ONC with further development of the Direct Trusted Agent Accreditation Program, and the establishment of a national trust anchor bundle distribution service for Direct exchange implementers.

The problem Direct exchange is designed to help solve - fragmentation

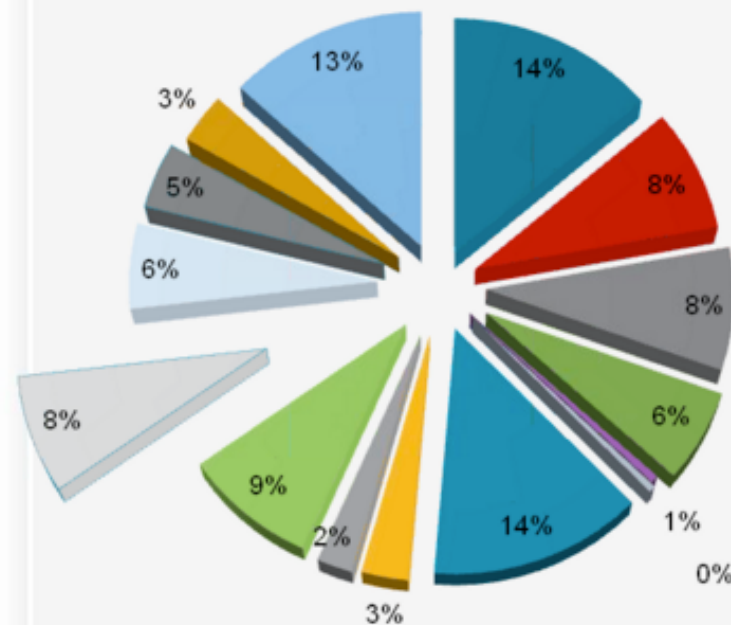


Example of HIT Fragmentation in One County (actual data)

near Phoenix, Az.

- **6400+** physicians using **70+** EHR vendors
- **58** of these vendors representing fewer than 100 physicians each
- **8%** of this county's physicians using Epic (2 IDNs)
- **104+** Walgreens and **64+** CVS pharmacies**
- **8 HIEs** and the Immunization Information System (IIS) State Registry
- **Diagnostic imaging** centers, **lab** information systems, and **long term care** providers

Estimated Number of Physicians by EHR Vendor in Example County*



*Source: DirectTrust e-prescribers used as a proxy to estimate physicians in the county. County used as a proxy to define region.
**Source: Walgreens and CVS online store locations, regions: Florida, Georgia, Illinois, Colorado, and Texas
***Source: <http://www.healthdata.gov/data-act/2014-09-01>

Direct exchange: it's not just about Stage 2 MU requirements



- Direct exchange is well suited to replace fax, e-fax, mail, and proprietary connections:
 - Between providers during transitions of care;
 - Between providers and patients;
 - Between federal and state agencies and providers for document exchange, requests for information;
 - Between payers and provider organizations;
 - Between patients and patient applications for organization, display, reconciliation, analysis.

DirectTrust is an outgrowth of the Direct Project “Rules of the Road” WG



X.509 Certificate Policy Established
December 2011



Accreditation Program Kick-off
February 2013



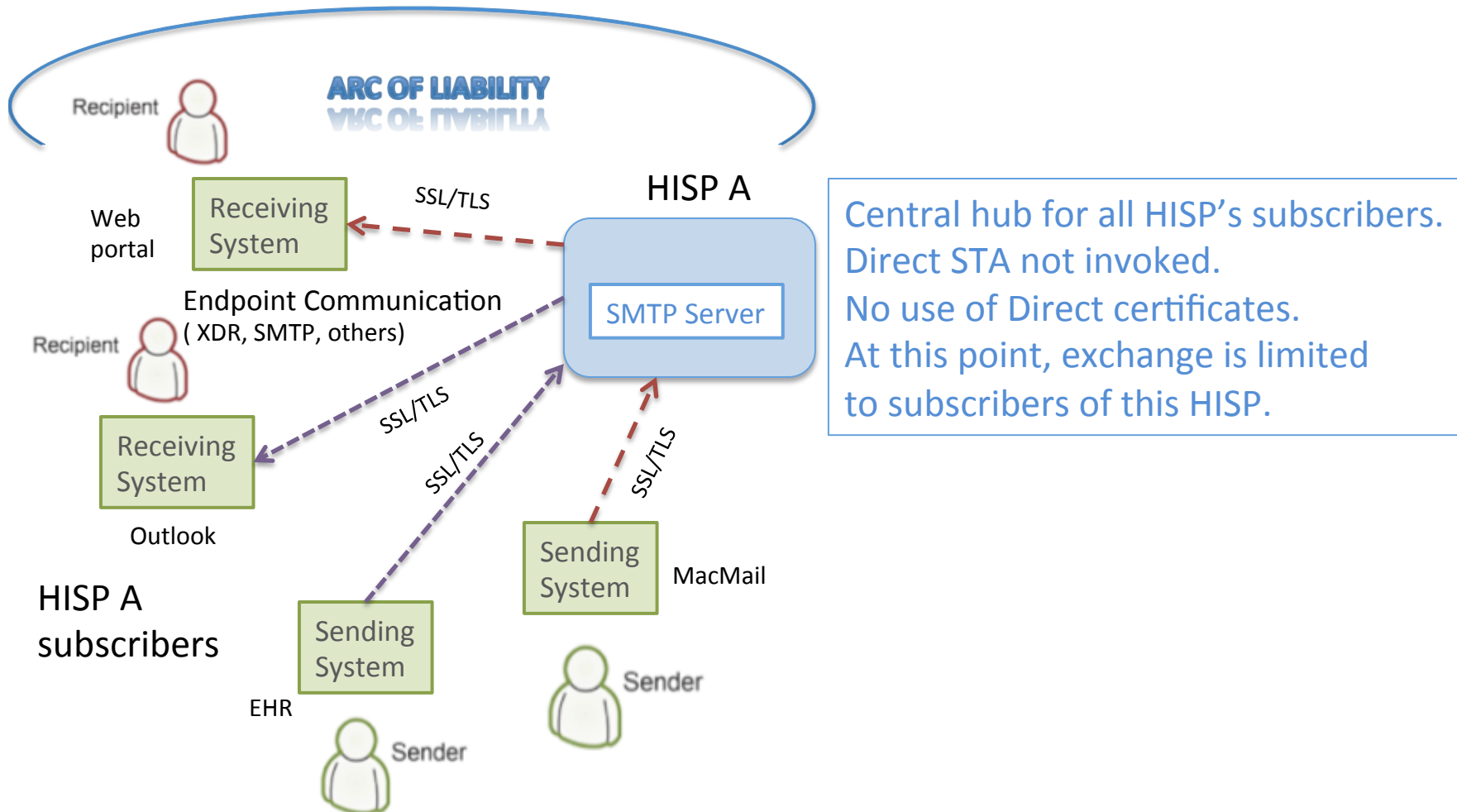
ONC Cooperative Agreement Award
March 2013



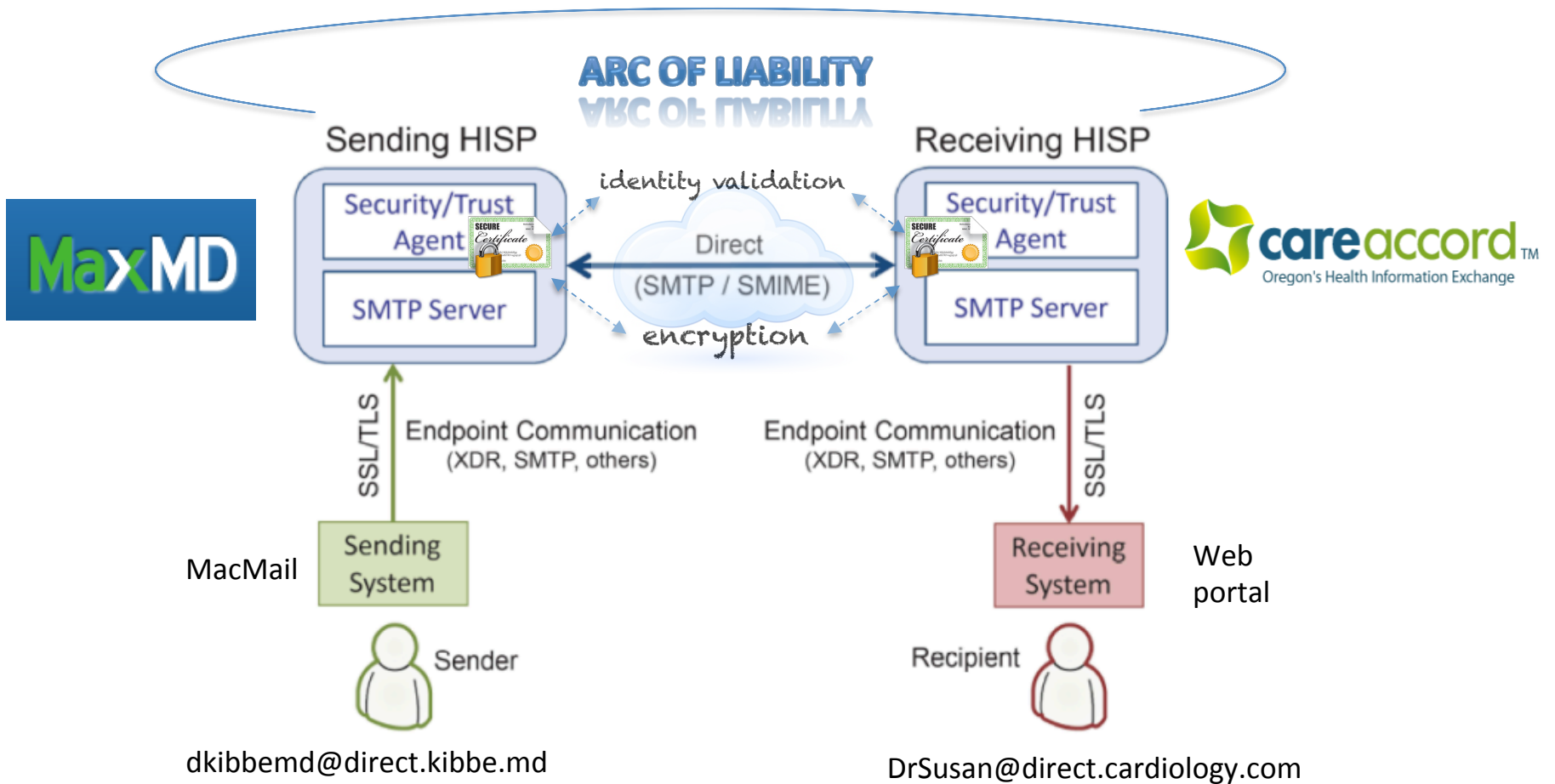
Trust Anchor Bundle Distribution Service Starts
May 2013

- DirectTrust’s membership includes over 80 entities, including state HIEs and state agencies, coalitions, HISPs, EHR vendors, provider groups, certificate authorities, consultants, and private individuals.
- DirectTrust members are serving Direct users/subscribers in all 50 states as HISPs, CAs, and RAs within the context of Stage 2 Meaningful Use, and beyond.
- DirectTrust is the only national Security and Trust Framework provider for Direct, and in partnership with EHNAC, the sole accrediting body for Direct trusted agents – HISPs, CAs, and RAs.

How it works: Single HISP exchange is Email via an encrypted session



HISP-HISP Direct exchange adds in a layer of security & trust in order to enable *point-to-point* exchange between subscribers of *different* HISPs, over the Internet, *without* a central hub.

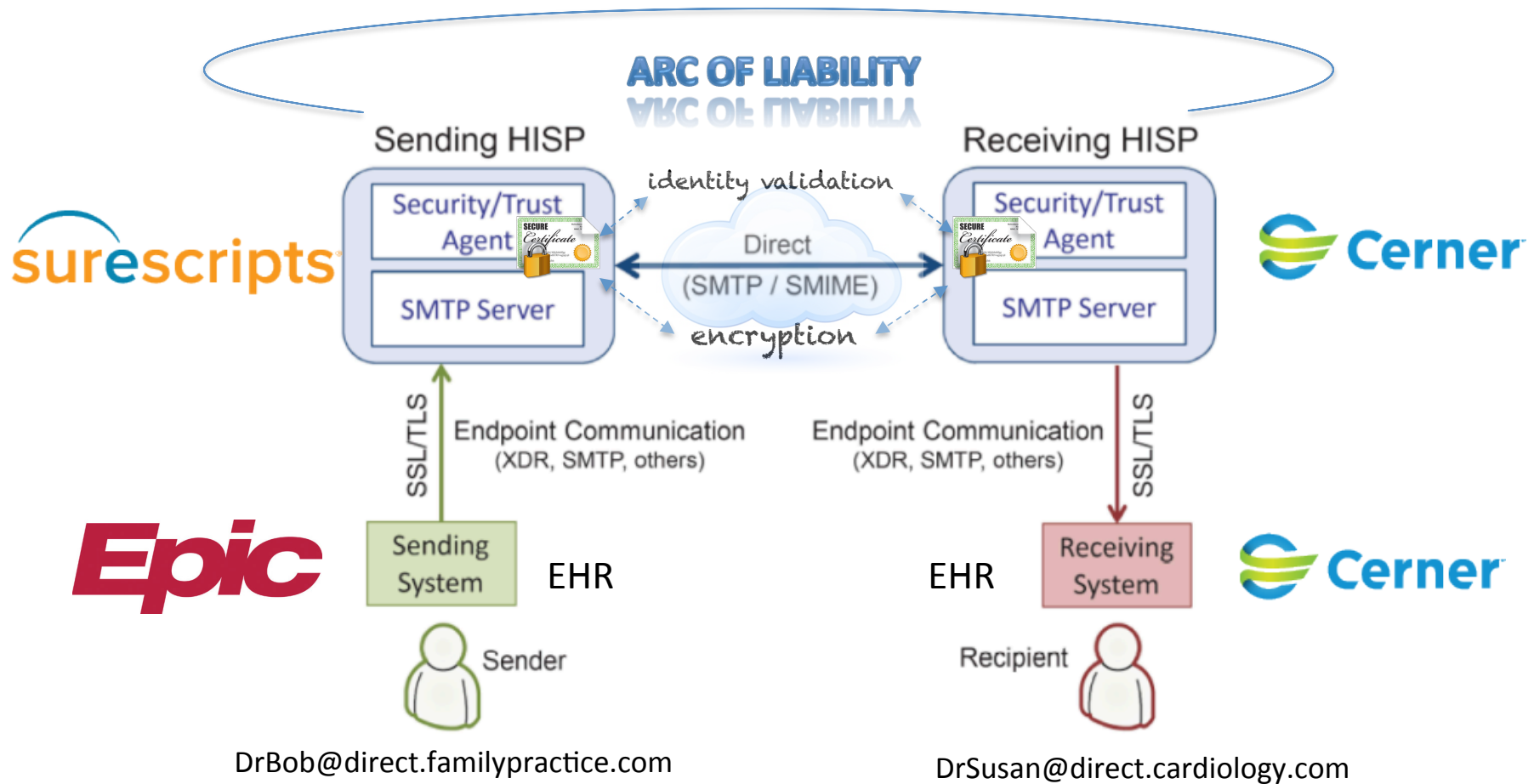


HISP definition

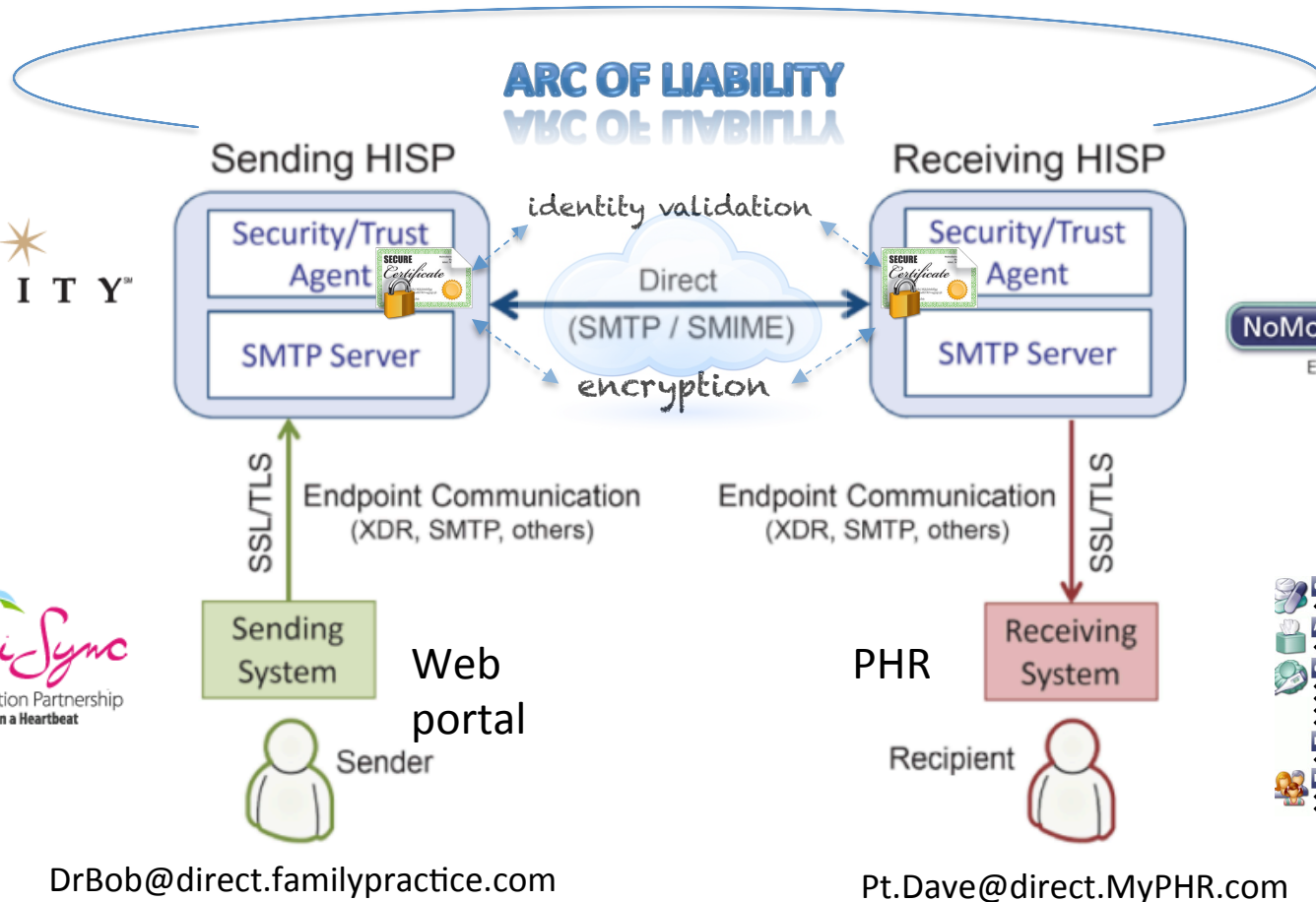


- In order for there to be Direct services, there must be a Health Information Service Provider, HISP.
- A HISP is an entity that conducts the secure transmission of Direct messages to and from Direct Addresses, each of which is bound to a Direct X.509 digital certificate (i.e. provides “Direct Services”).
- A HISP must act in the capacity of a Business Associate or Contractor for the Customer, in which case the HISP may hold and manage PKI private keys associated with Direct digital certificates on behalf of the Customer’s users/ addressees.
- A HISP may be a part of a larger organization that offers and performs services that are beyond the boundary of the HISP’s roles and responsibilities.
- A HISP does NOT use, manage, analyze, or otherwise perform actions upon the information transmitted and made secure.

HISP-HISP between EHRs



HISP-HISP exchange between EHR and PHR



- Current Medications [Edit]
 - Zolof 50mg (Every morning)
- Allergies [Edit]
 - PENICILLIN (Swelling)
- Current Illnesses [Edit] [Conditions Review]
 - Chronic Sinus Infections (Birth)
 - Hayfever (Birth)
 - Malignant Melanoma (07/01/2000)
 - Sinus Problems (Birth)
- Illness History [Edit]
 - Basel Cell Cancer(2007-01-05 14:33:01)
- Family Medical History [Edit]
 - High blood pressure (Grandparent)
 - High blood pressure (Mother)

Questions



- How does HISP A know that HISP B...X,Y,Z are trustworthy enough to exchange HISP's subscribers' Personal Health Information with them? What are the risks?
- How does HISP A establish a baseline of assurance regarding security and trust-in-identity with HISP B...X,Y,Z ? A baseline that will scale?
- What mechanisms are available for HISP A to signal its trustworthiness to others, efficiently and at scale?

Building a Network via Bi-directional Contracts is Unworkable



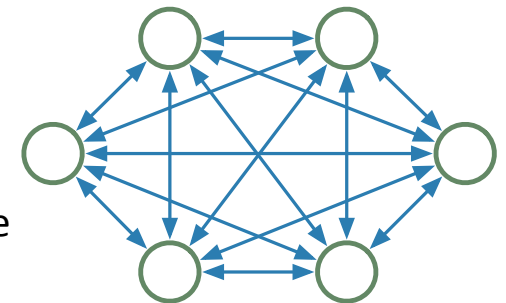
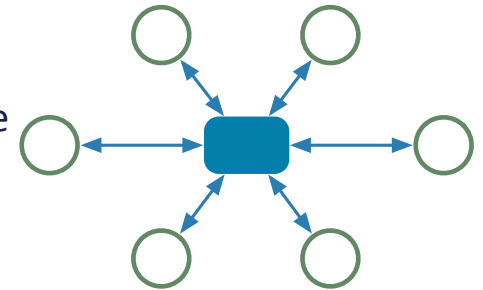
- If HISPs choose to negotiate the “rules of the road” with each other one at a time, forging one-off contracts, the cost of Directed exchange goes up with each new HISP contract. Complex. Rate limiting. Will not scale.



Scalable Trust and the N-squared problem



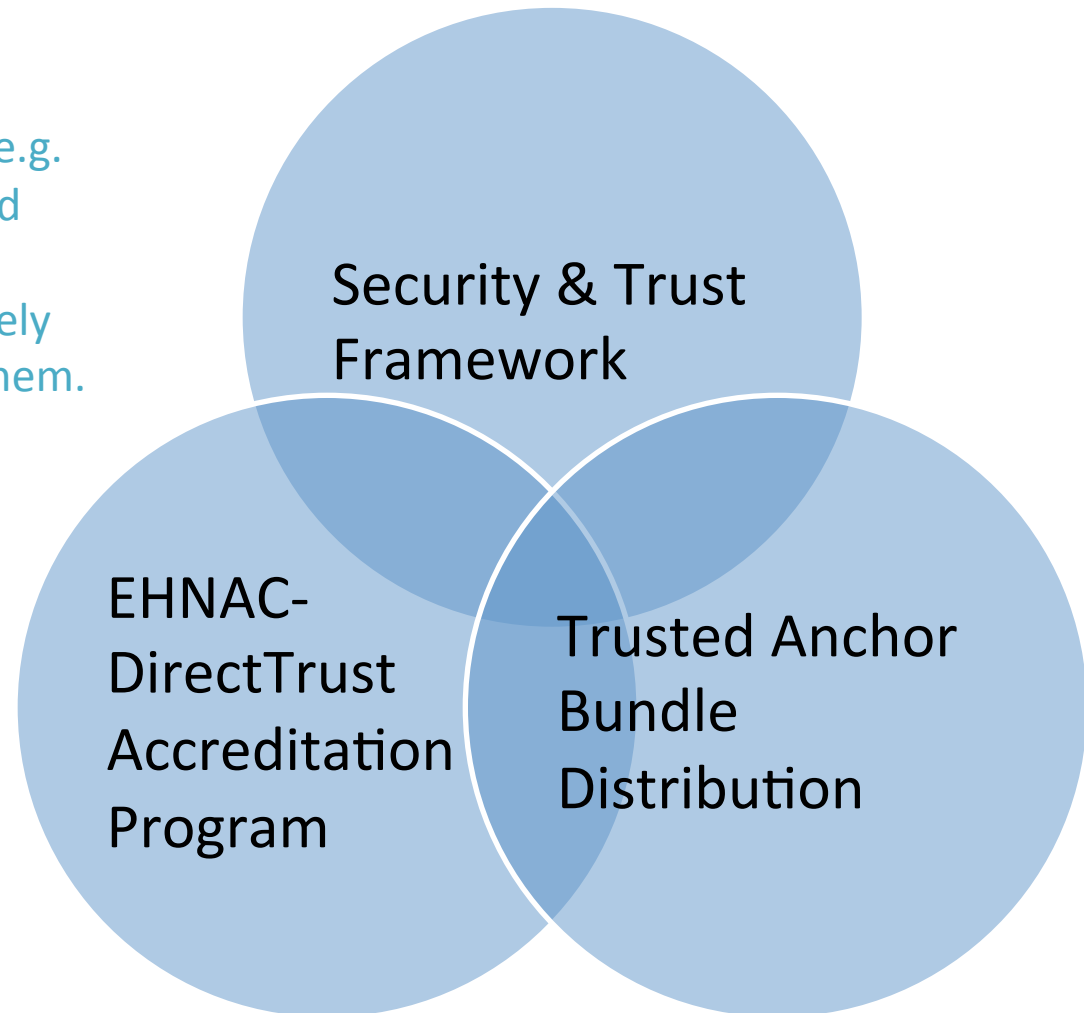
- Scalable Trust is a strategy for enabling Directed exchange between a large number of endpoints, in this case HISPs and their users/ subscribers.
- If “scalable,”
 - Trust should happen “quickly” and uniformly.
 - A “complete” network will be formed voluntarily.
 - Complexity and cost of establishing a network will decrease, while the value of the network itself will increase, as more nodes are added.
 - This “network effect” will be a by-product of making trust scalable.
 - Eliminates the need for one-off manual business agreements and technical connections.
- If not “scalable,”
 - Parties will be forced to create one-off manual business agreements and technical connections increasing cost and complexity.
 - Manual exchange and maintenance of trust anchors doesn’t scale beyond the smallest of numbers – N-squared problem.



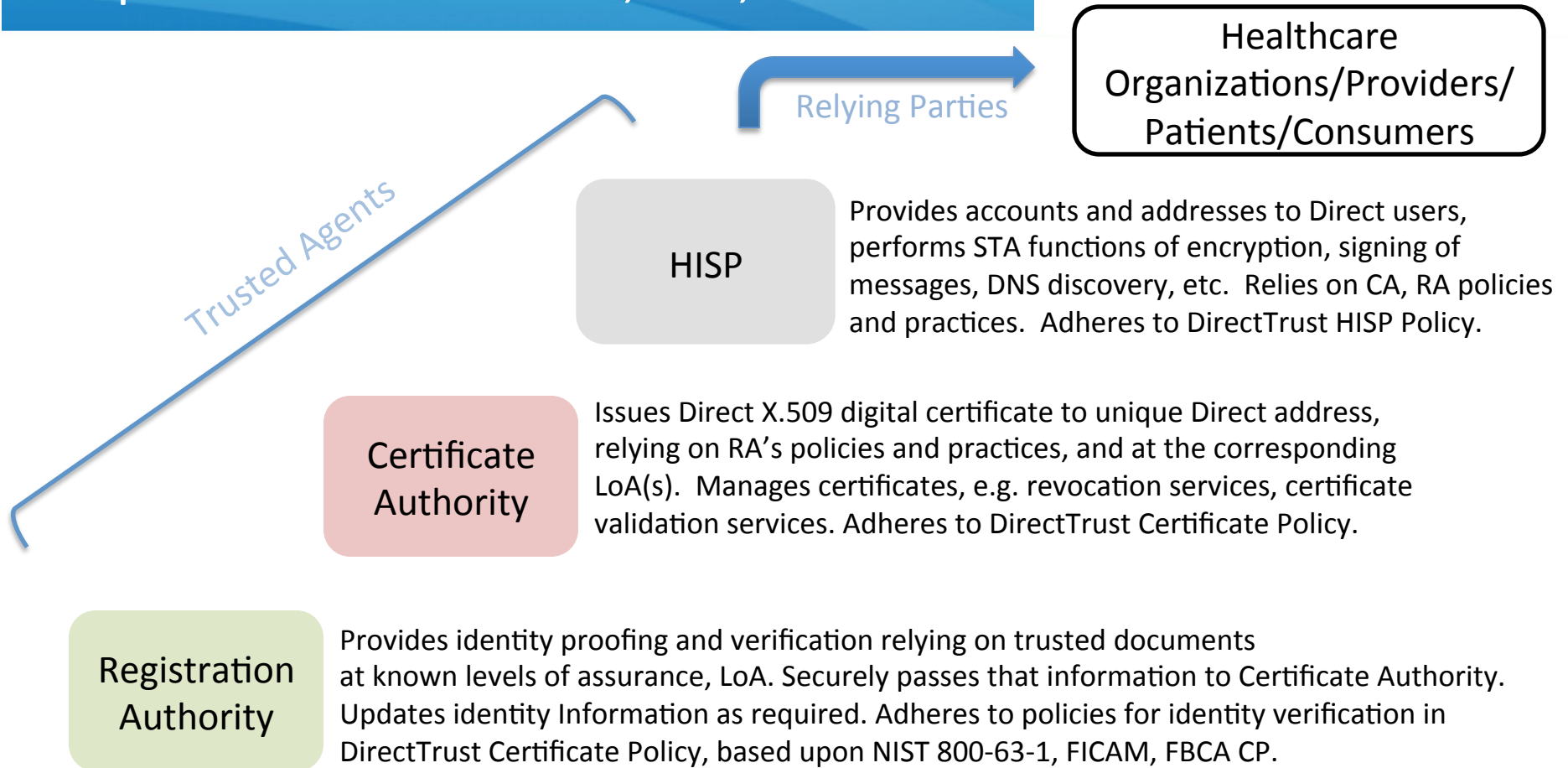
DirectTrust Approach



The goal is to make it easy and inexpensive for trusted agents, e.g. HISPs, to voluntarily know of and follow the “rules of the Road,” while also easily and inexpensively knowing who else is following them.



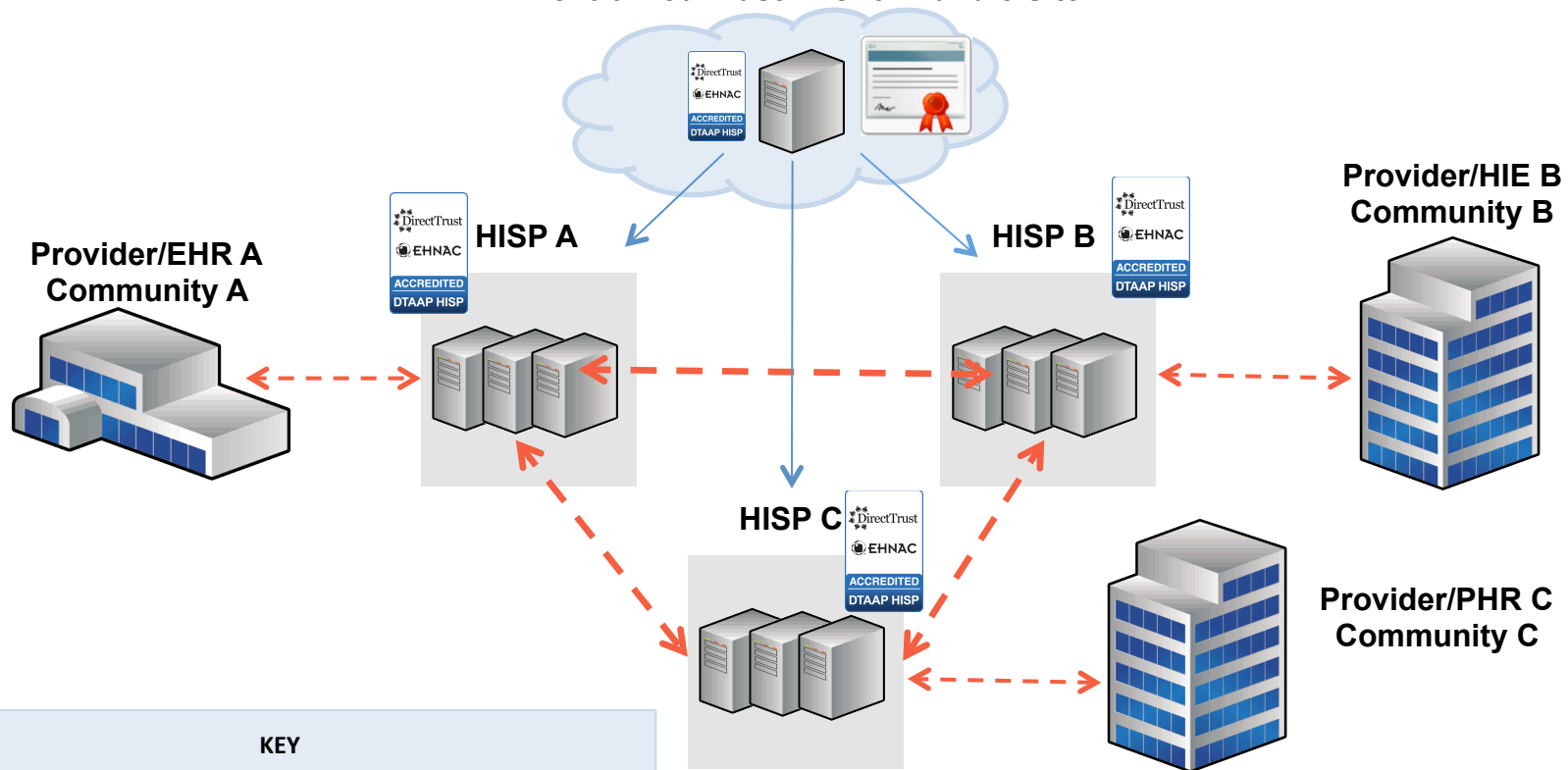
Trusted agents: key roles and responsibilities for HISPs, CAs, RAs



Example of the DirectTrust Community's "Scalable" Trust



Centralized Trust Anchor Bundle Site




KEY

--- Trust relationship based on accreditation

DirectTrust Approach



Avoid this:



The site's security certificate is not trusted!

You attempted to reach 1.1.1.1, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

[▶ Help me understand](#)

With this:



Resources and additional information



- DirectTrust website www.DirectTrust.org

[Information on Membership](#)

[Information on Workgroups and Active Projects](#)

[DirectTrust Membership List](#)

[Accreditation Status List](#)

[Code of Ethics](#)

[DirectTrust Community X.509 Digital Certificate Policy](#)

[Federation Agreement](#)

[Direct Trusted Agent Accreditation Program \(DTAAP\)](#)

[Trust Anchor Bundle Website](#)

David.Kibbe@DirectTrust.org