Overview of Obvious Solutions Inc's

Secure Messaging Solutions for eBusiness

Derek Ritz, P.Eng.
Chief Technology Officer

Obvious Solutions Inc.

abrica™ dabra

Obvious Security Platform™

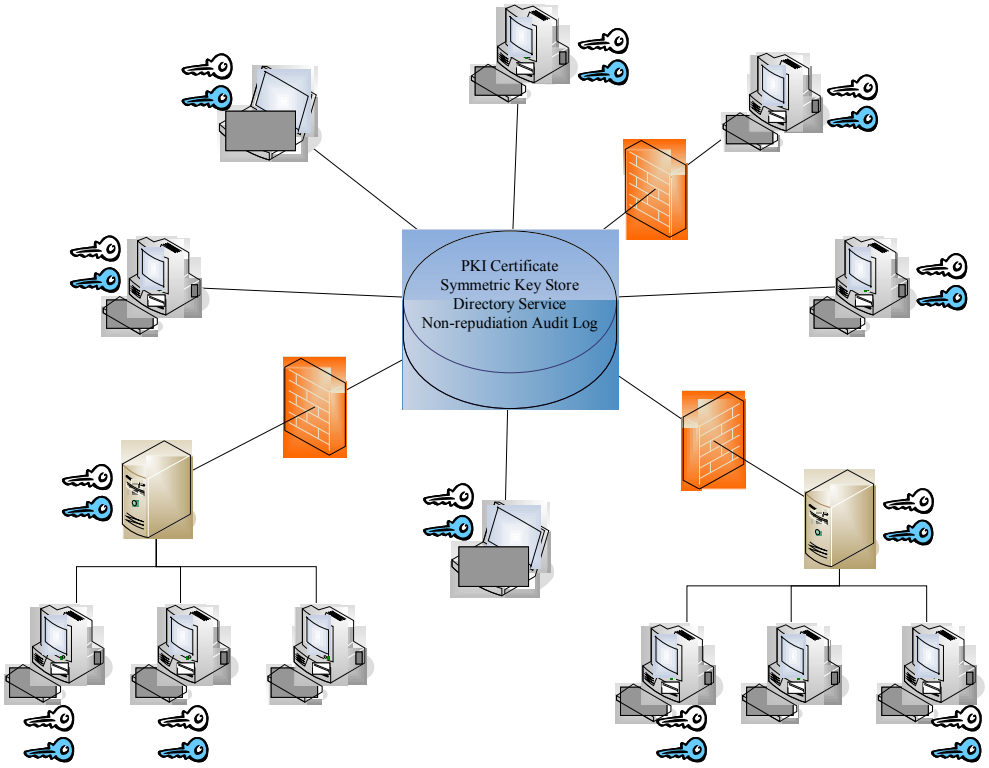
- Obvious Solutions Inc. is a privately held Canadian technology company providing secure collaboration solutions for eBusiness.
- Obvious has developed a patent-pending security platform that provides a cryptographically hardened infrastructure which can be deployed easily and inexpensively across the Internet and other Internet Protocol (IP) based networks.
- The Obvious Security Platform supports multiple business applications offered as secure services over open IP based networks.
- Obvious currently has two such services offerings:
  - Abrica, for simply and securely exchanging structured documents (Purchase Orders, Shipping Notices, Claims Forms, Invoices, etc.) between business partners using disparate business management systems
  - Dabra, for the secure, seamless exchange of e-mail and file attachments between individuals

Obvious Security Platform™

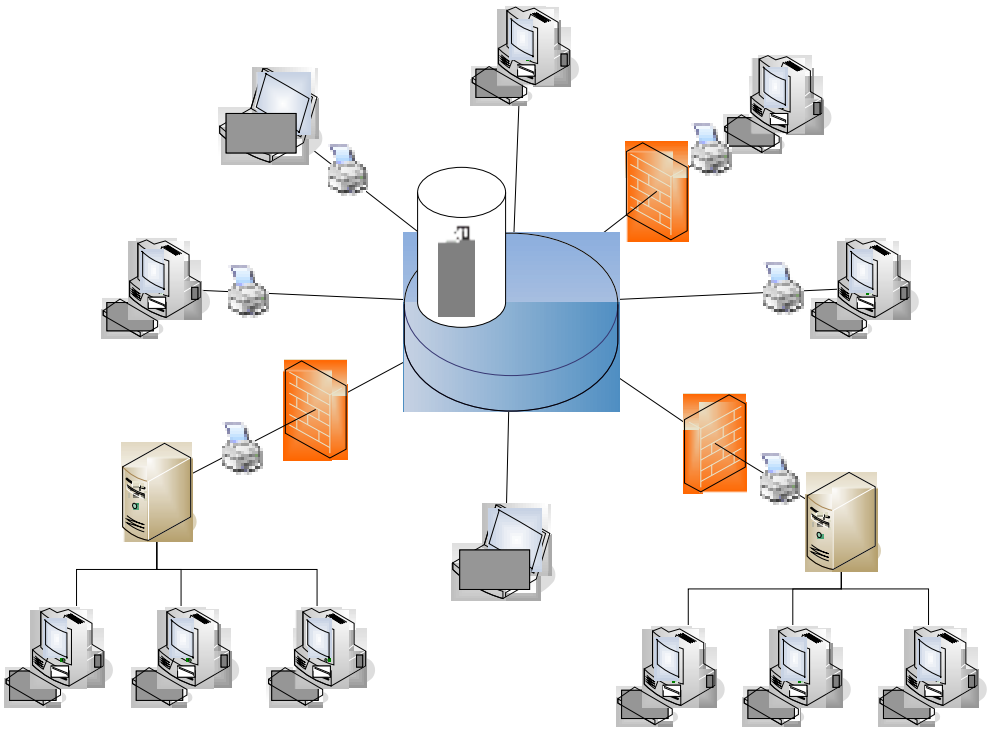
abrca™ dabra

Obvious Security Platform™

- The Obvious Security Platform provides an Internet-based infrastructure for the secure exchange of messages between parties
- The platform employs a unique, patent-pending hybrid architecture based on standard symmetric (AES 128bit) and asymmetric (PKI 1024bit) cryptography
- PKI certificates are not needed for each member node on the platform; a PKI certificate is only required at the central Notary Server
- Messages sent over the network create a non-repudiation audit trail including: authenticated sender & receiver, send & receipt notary timestamps, and digital fingerprints (hashes) of the message contents.
- The network does not depend on border security (firewall) technologies; the system transparently works with or without a firewall



- Abrica is a "printer" façade software client that may be used by companies to send and receive structured business documents using the Obvious Security Platform
- Each company that participates in an Abrica transmission is authenticated by a unique symmetric key
- Abrica works with any ERP or business management system
- To send a document to an authenticated recipient company, a user simply prints it to the Abrica "printer"
- The Abrica façade program intercepts the printer data stream and creates both a PDF and XML version of the document. These files are securely transmitted to the authenticated recipient via standard email, creating a non-repudiation audit trail at the Notary Server
- Abrica's unique and novel document mapping and parsing technology is patent-pending

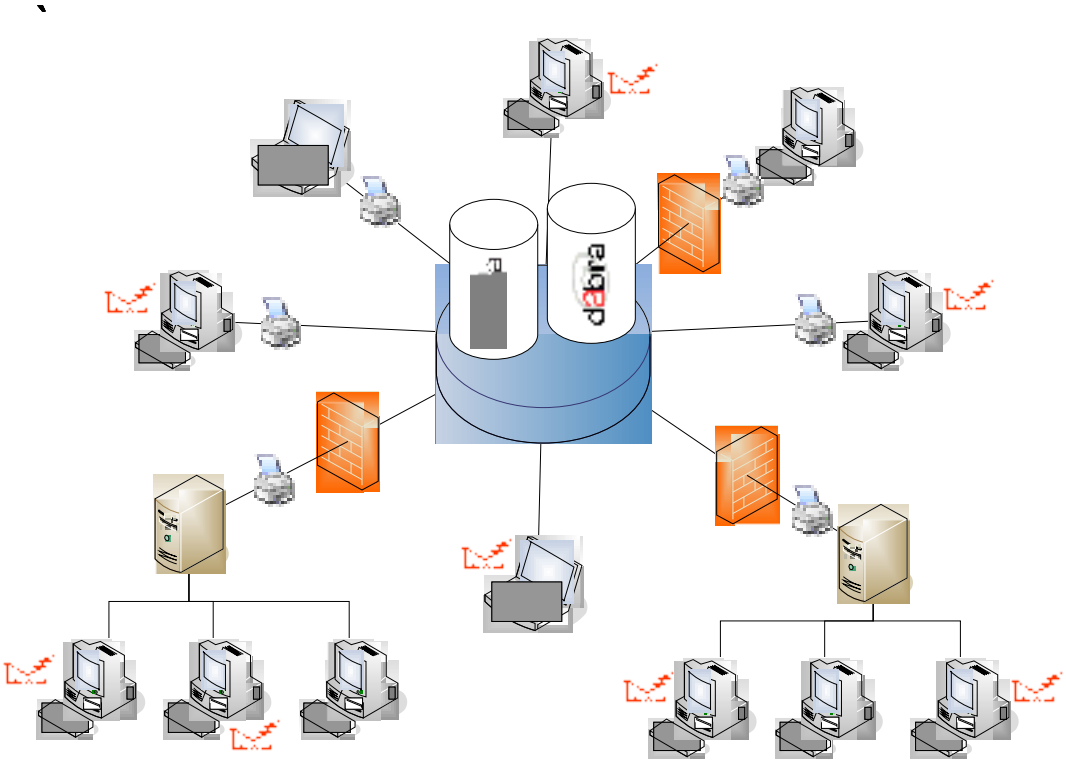


Dabra™

abrica™ dabra

Obvious Security Platform™

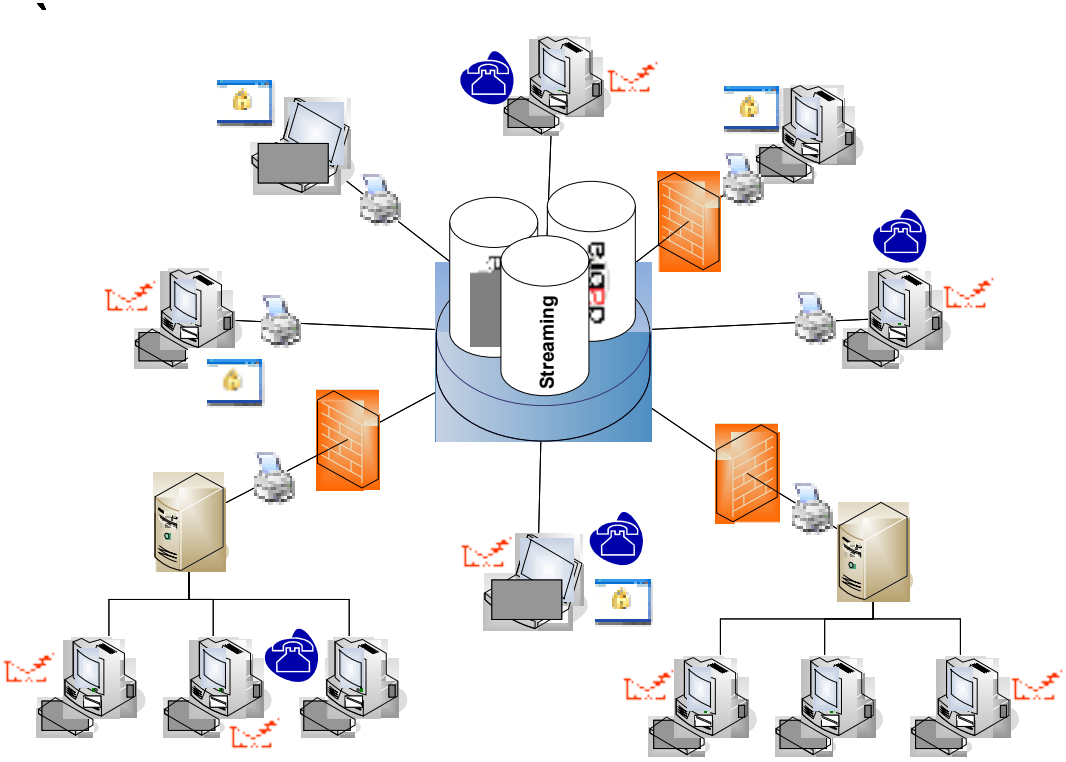
- Dabra is an email "plug-in" that supports encrypted messaging using the Obvious Security Platform
- Each individual email account is authenticated by a unique symmetric key
- Every message transmission authenticates the sender and the recipient, and creates a non-repudiation audit log at the notary server
- To send a message using Dabra, the user simply clicks the "Send Secure" button on their email program instead of the regular "Send" button
- Dabra's unique and novel key management and authentication method is patent-pending



Streamed Content Solutions

abrica™ dabra
Obvious Security Platform™

- The Obvious Security Platform can be used to deploy other secure business solutions.
- New solutions are contemplated by a recently filed patent application which extends the original technology to include secure, authenticated exchange of streamed content as well as discrete messages.
- Such new solutions could include:
  - Secure remote desktop or VPN connections
  - Secure connections over wireless 3G networks
  - Authenticated, encrypted voice-over-IP
  - Applications involving streamed video-over-IP



How Does it Work?

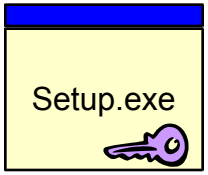
abrica™ dabra
Obvious Security Platform™

- How is key management accomplished?
- How are messages securely transmitted between parties?

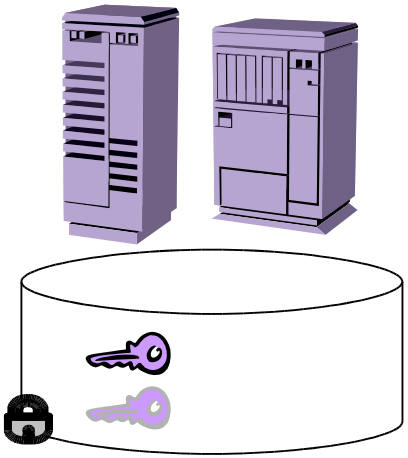
How Does it Work?

abrica™ dabra

Obvious Security Platform™

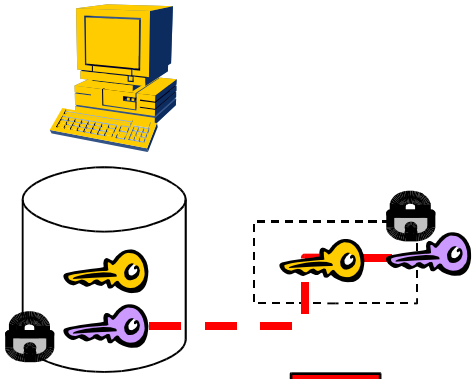


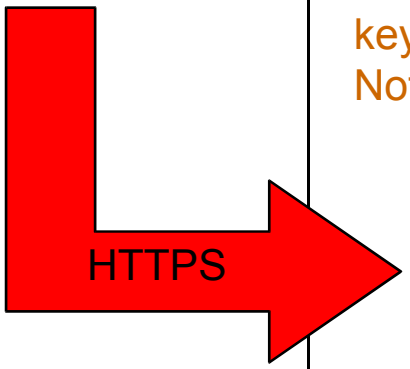
Orange and Blue wish to collaborate securely. Orange downloads a setup.exe program from the Internet, which contains the Notary Service's public key.

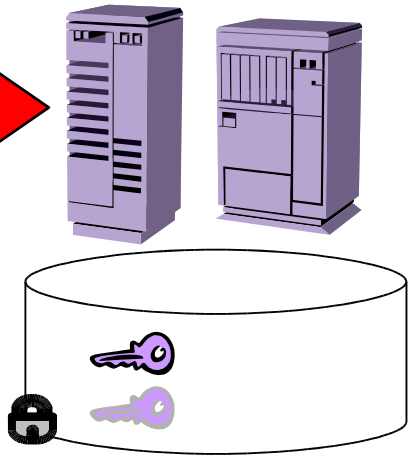


How Does it Work?

abrica™ dabra
Obvious Security Platform™



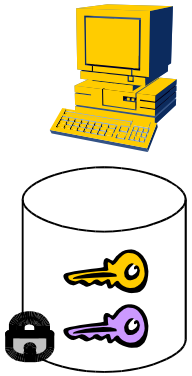




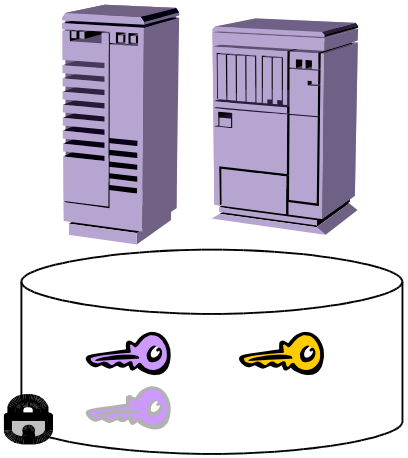
As a last step in the program's installation process, Orange generates and securely stores its own unique symmetric key, encrypts it with the PKI public key, and sends it to the Notary Service.

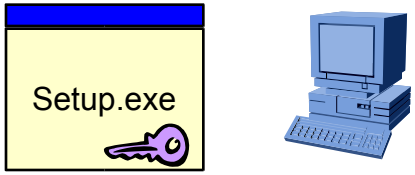
How Does it Work?

abrica™ dabra
Obvious Security Platform™



Now Orange has a shared secret with the Notary Service. To join the secure network, Blue also downloads and runs the setup.exe program.

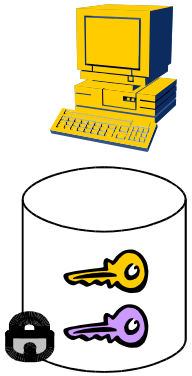




How Does it Work?

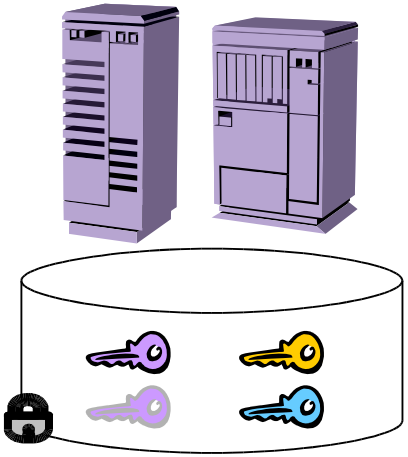
abrica™ dabra

Obvious Security Platform™

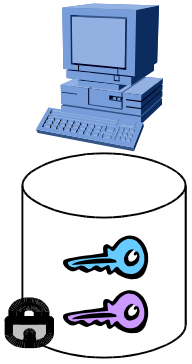


The sender, Orange, has his private “ID” key (orange key) and Notary Service’s PKI public key (dark purple) in a secure local data store.

The Notary Service has its PKI private key (light purple) and public key (dark purple) in a local secure data store. The Notary Service maintains a copy of each subscriber’s “ID” key in it’s secure database (orange key, blue key, etc.). Each key is associated with a unique entity. For Abrica, there is one key per company. For Dabra, one key per email address..



The receiver (Blue) has his private “ID” key (blue key) and Notary Service’s PKI public key (dark purple key) in a secure local data store.

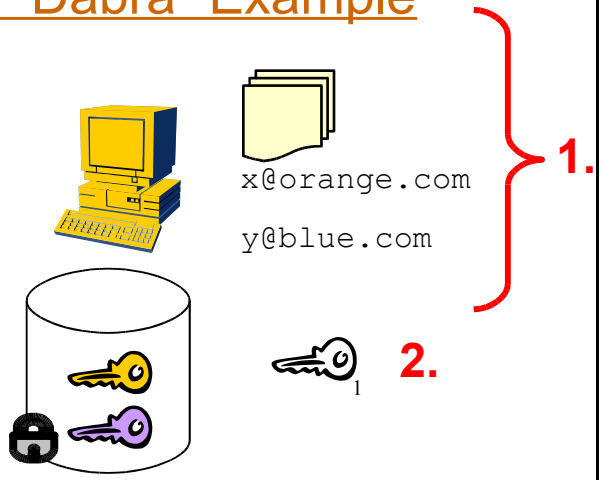


How Does it Work?

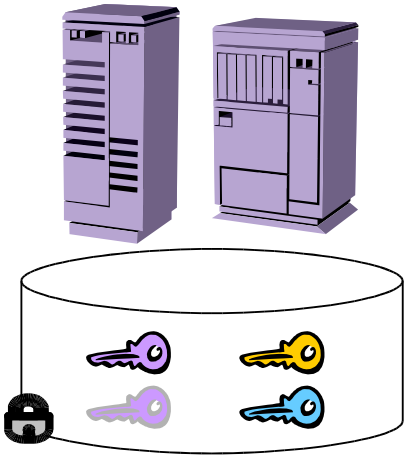
abrica™ dabra

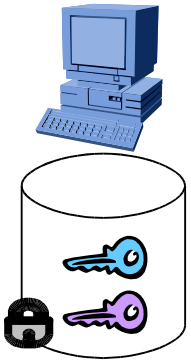
Obvious Security Platform™

A "Dabra" Example



1. The sender email address, receiver email address and "payload files" are specified.
2. A unique , one-time "session" key (white key #1) is generated by the sender. This key will be used to encrypt the sender's communication with the Notary Service.

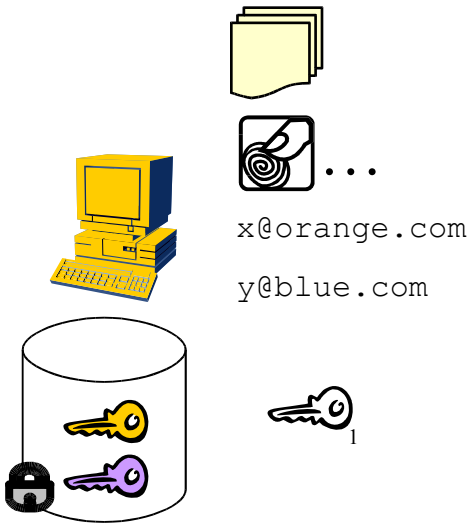




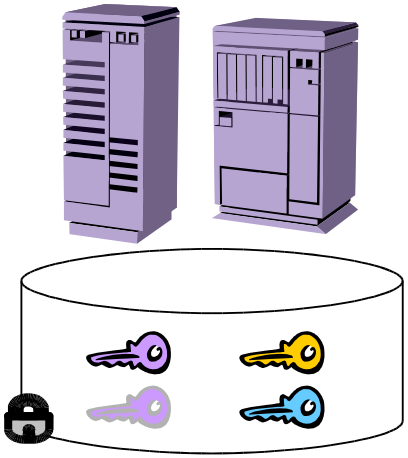
How Does it Work?

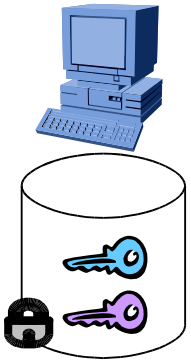
abrica™ dabra

Obvious Security Platform™



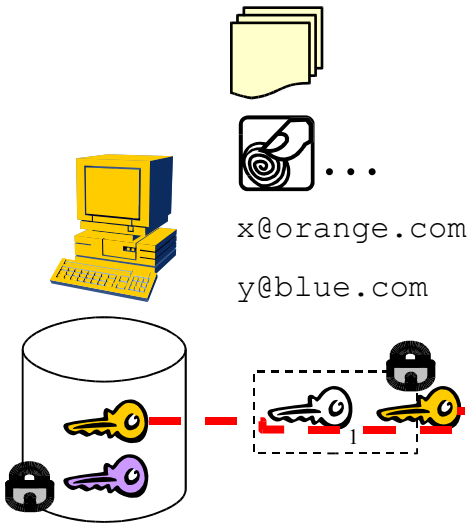
Digital fingerprints are created for each payload document.



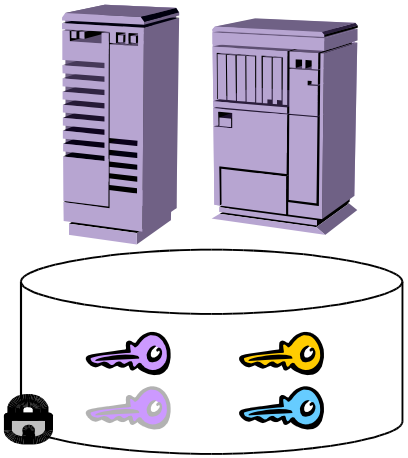


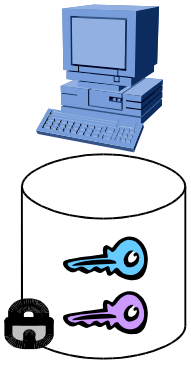
How Does it Work?

Obvious Security Platform™



To authenticate the sender, the session key is encrypted using the sender's ID key (orange key).

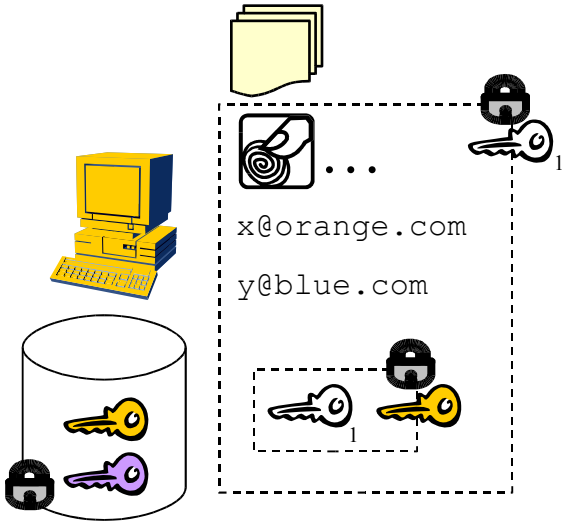




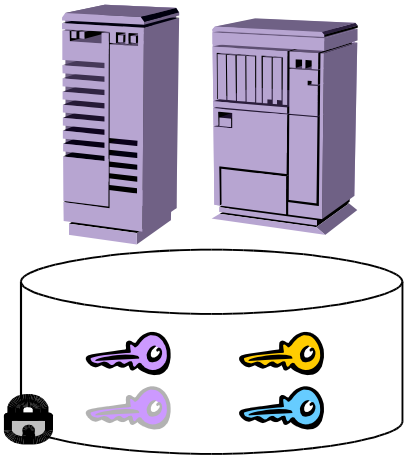
How Does it Work?

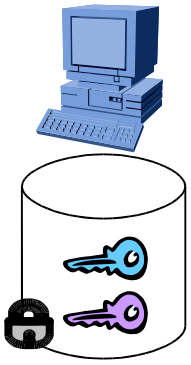
abrica™ dabra

Obvious Security Platform™



The email addresses and payload fingerprints are encrypted using the session key (white) and then zipped (to compress the size of the transmission).

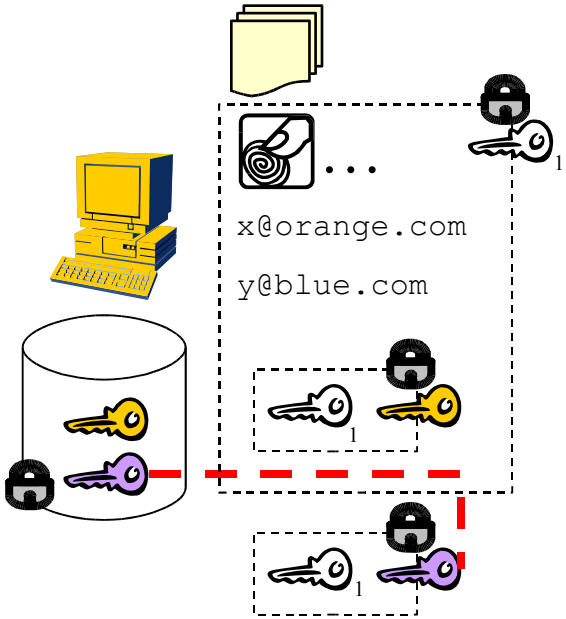




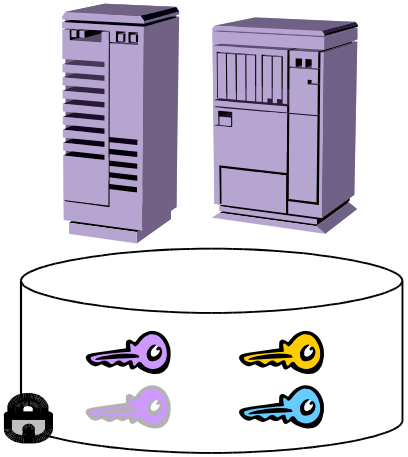
How Does it Work?

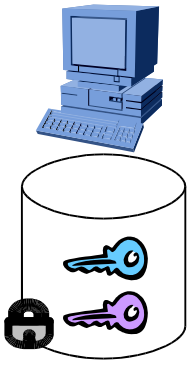
abrica™ dabra

Obvious Security Platform™



The session key (white) is encrypted using the Dabra PKI public key (dark purple).

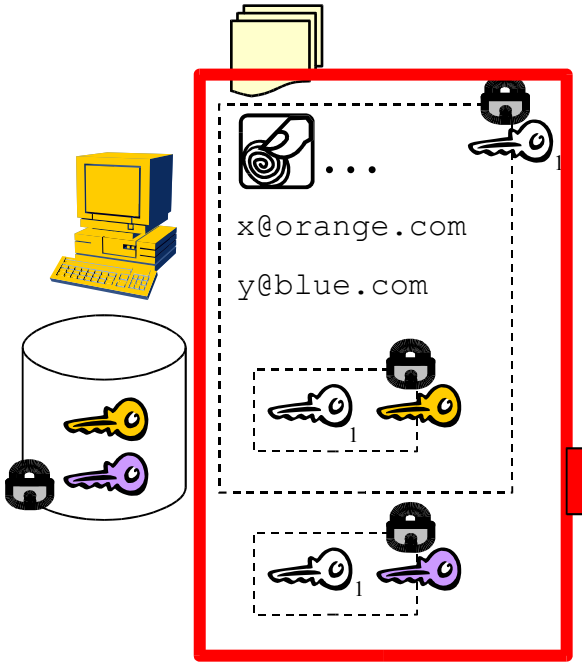




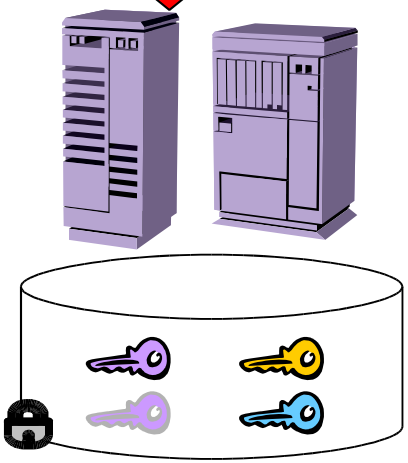
How Does it Work?

abrica™ dabra

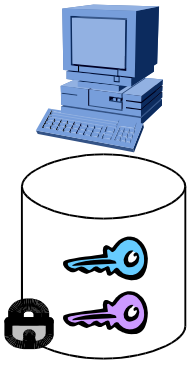
Obvious Security Platform™



HTTP

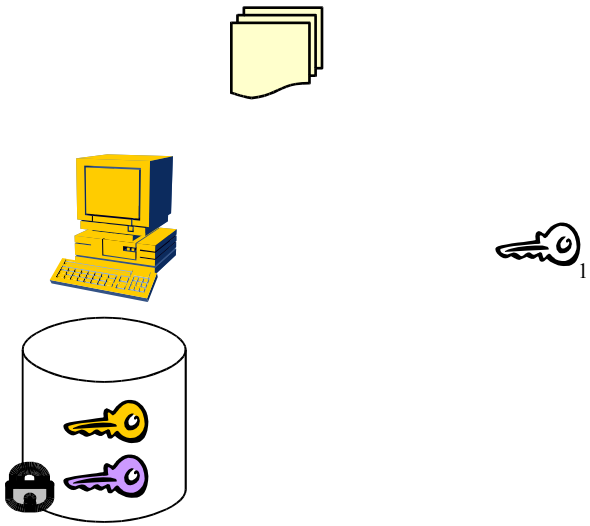


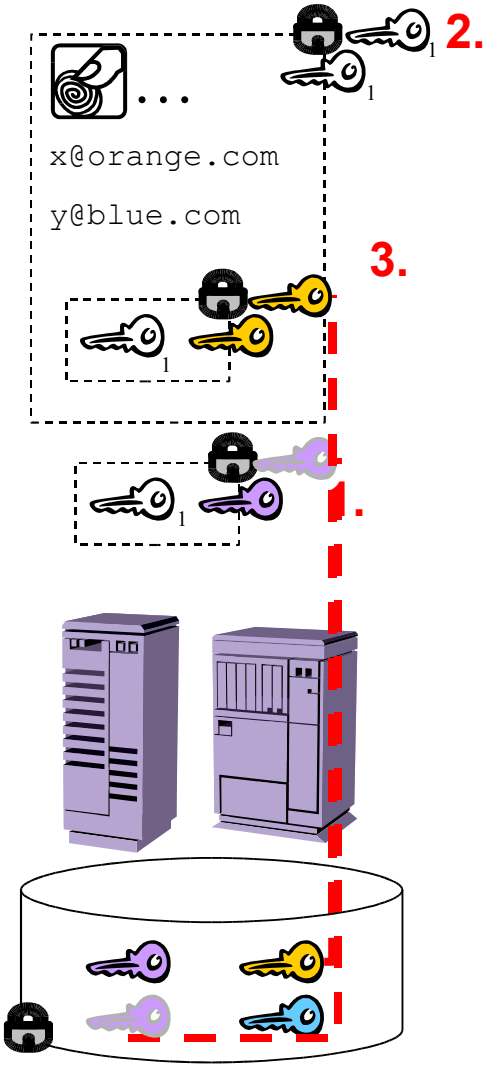
The package, including zipped payload plus encrypted session key, is posted to the Notary Service using HTTP. The sender keeps a copy of the session key for later processing of the HTTP reply message.



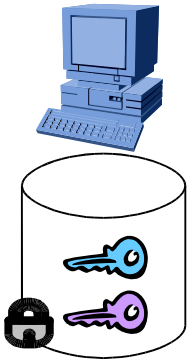
How Does it Work?

abrica™ dabra
Obvious Security Platform™



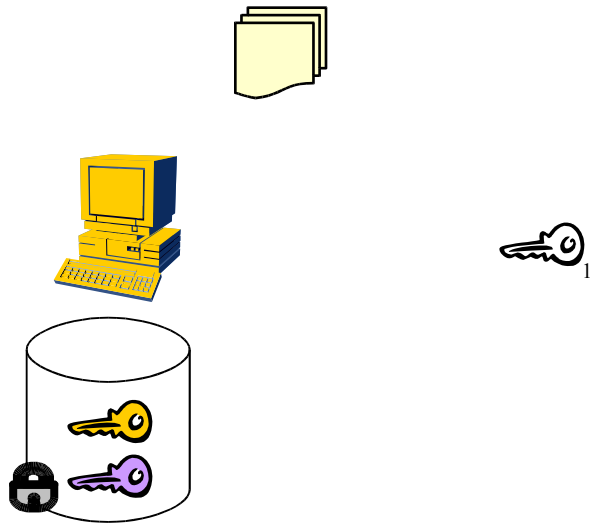


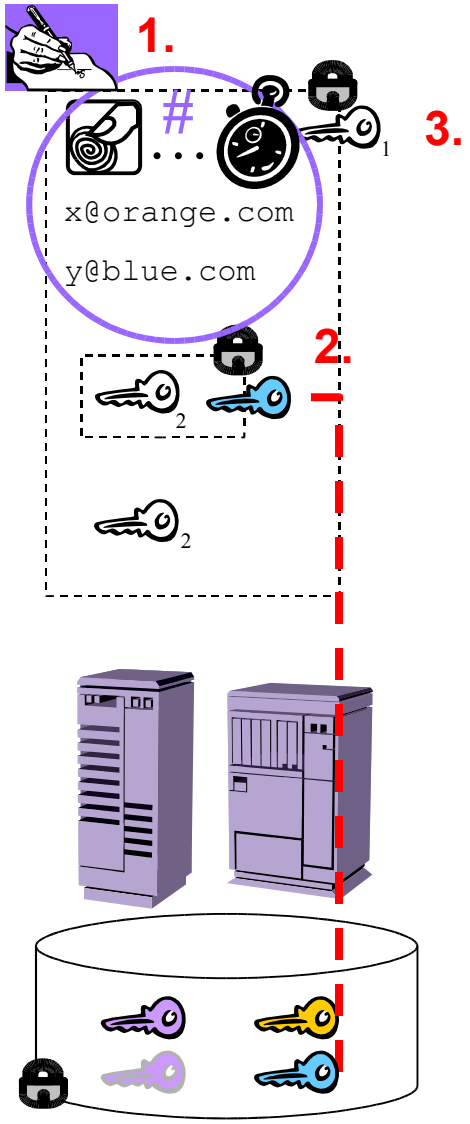
1. The Notary Service uses its private PKI key (light purple) to decrypt the session key (white).
2. The payload is unzipped. The session key (white) is used to decrypt the payload contents.
3. Based on the sender email address, the “ID” key of the purported sender (Orange) is retrieved and used to decrypt the session key, thus authenticating the sender.

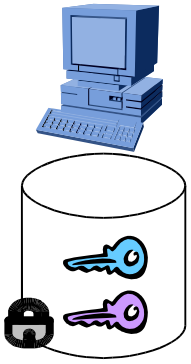


How Does it Work?

Obvious Security Platform™





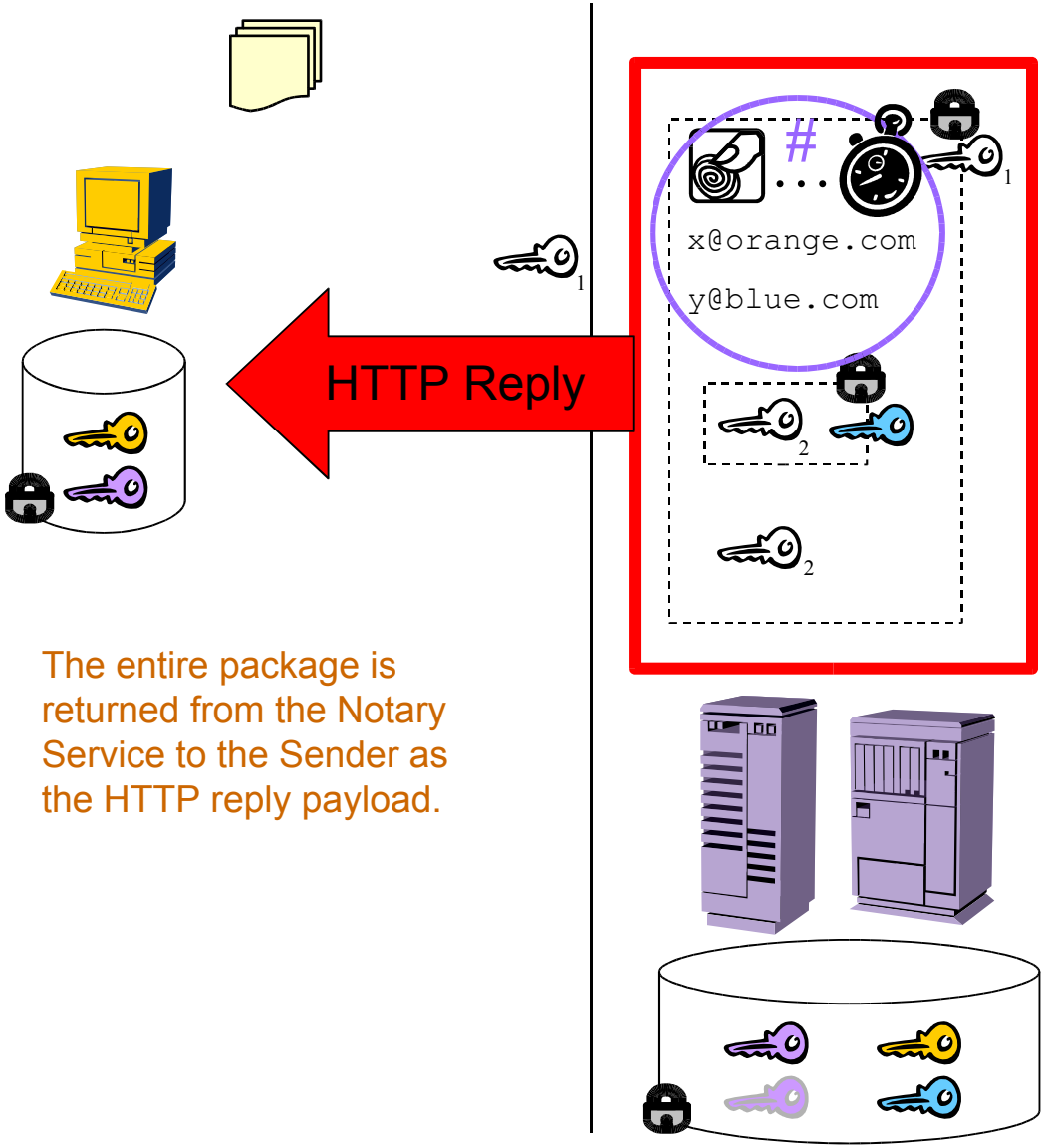


1. The Notary Service timestamps the transmission, assigns a transmission GUID, saves the audit info, and signs a copy of the content for return to the sender.
2. Using the receiver email address as a lookup, a 2nd session key is created and encrypted with Blue key.
3. An unencrypted copy of the 2nd session key is also included, and the entire reply payload is encrypted with the 1st session key.

How Does it Work?

abrica™ dabra

Obvious Security Platform™

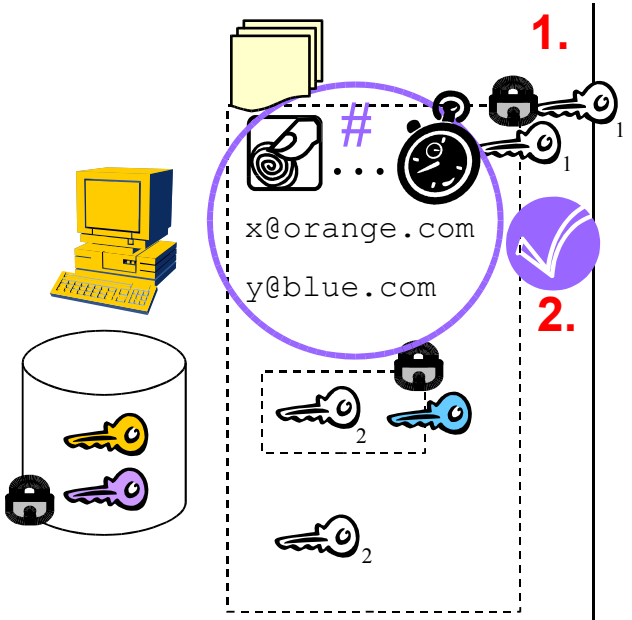


The entire package is returned from the Notary Service to the Sender as the HTTP reply payload.

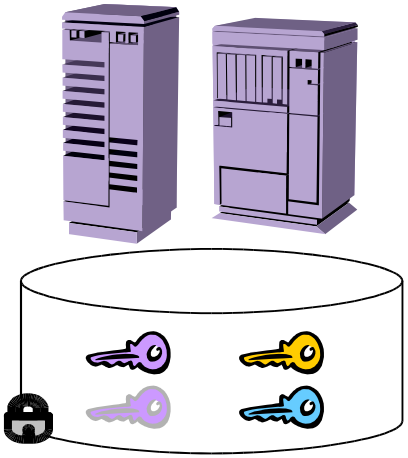
How Does it Work?

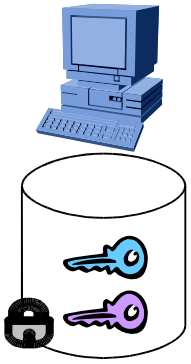
abrica™ dabra

Obvious Security Platform™



1. The saved 1st session key is used to decrypt the payload
2. The signed content is verified, authenticating it as having come from the Notary Service.

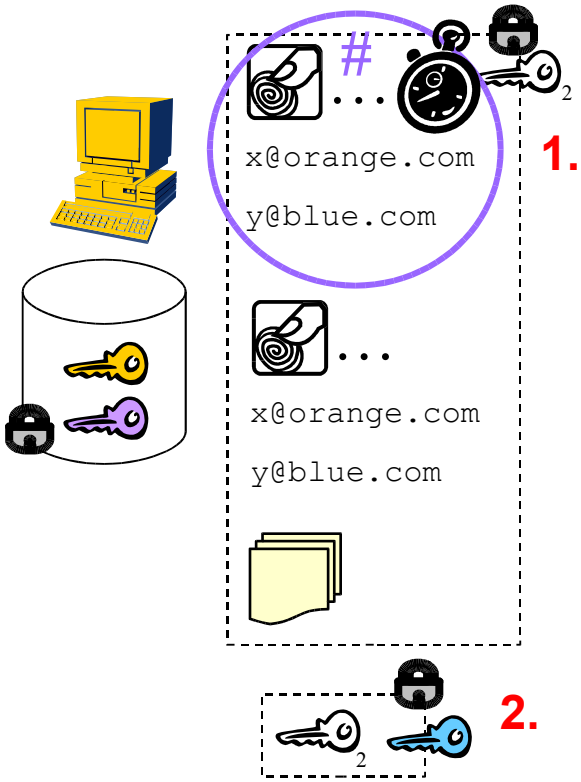


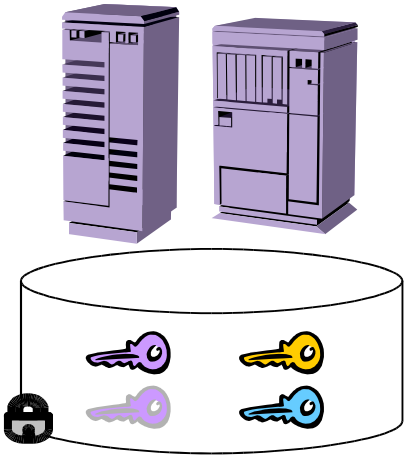


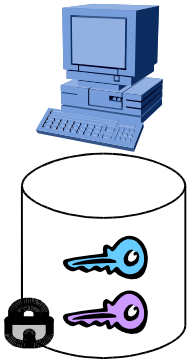
How Does it Work?

abrica™ dabra

Obvious Security Platform™





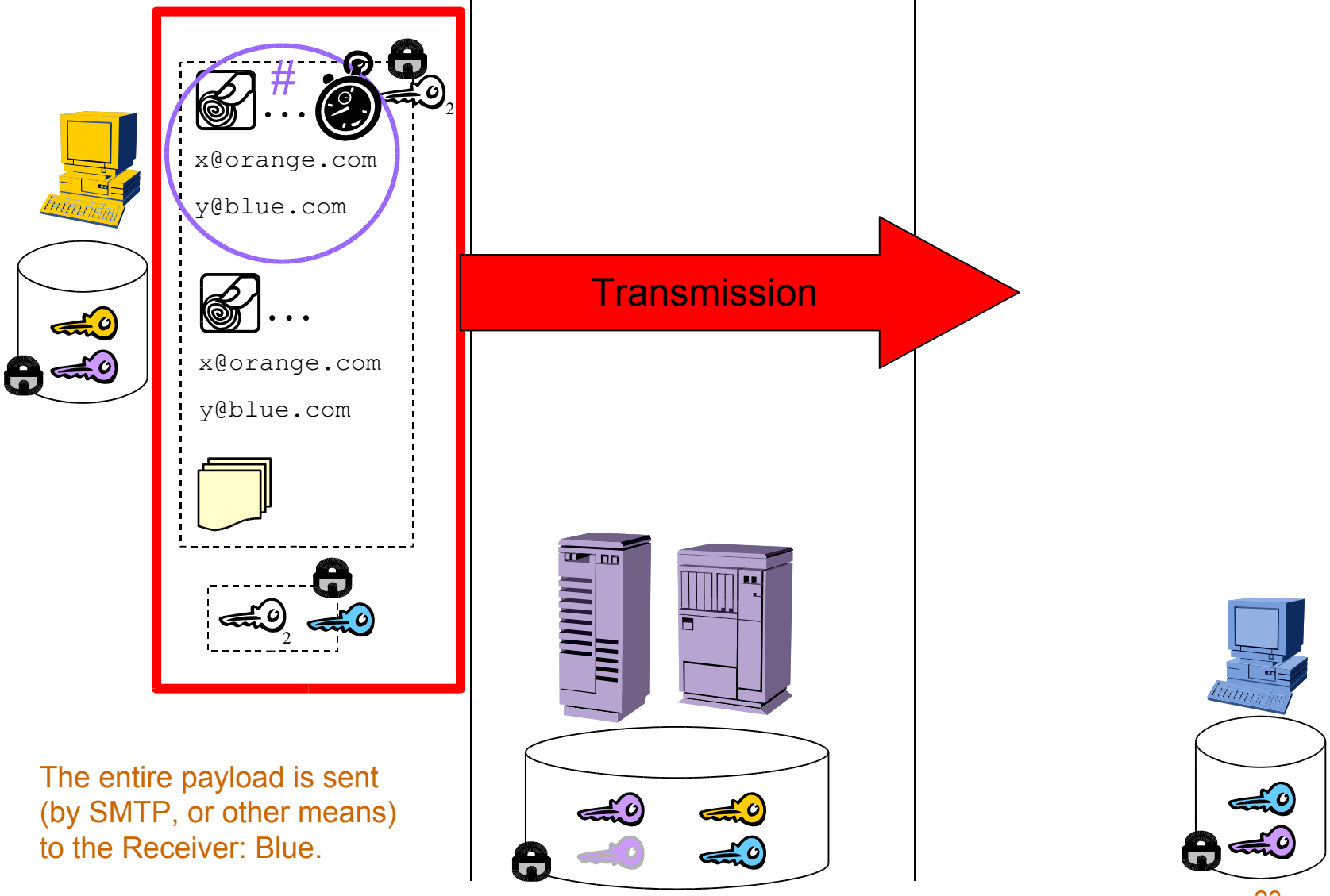


1. A final payload is constructed, including the signed content, and encrypted using the 2nd session key.
2. The Blue-encrypted 2nd session key is included

How Does it Work?

abrica™ dabra

Obvious Security Platform™

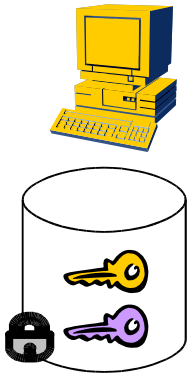


The entire payload is sent (by SMTP, or other means) to the Receiver: Blue.

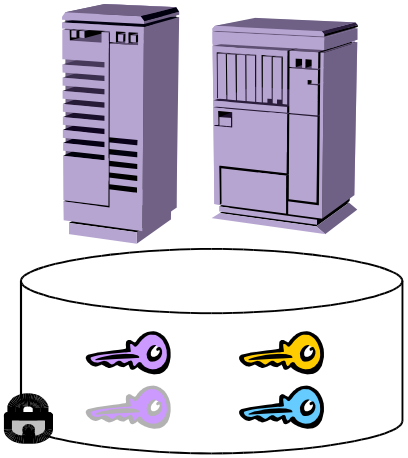
How Does it Work?

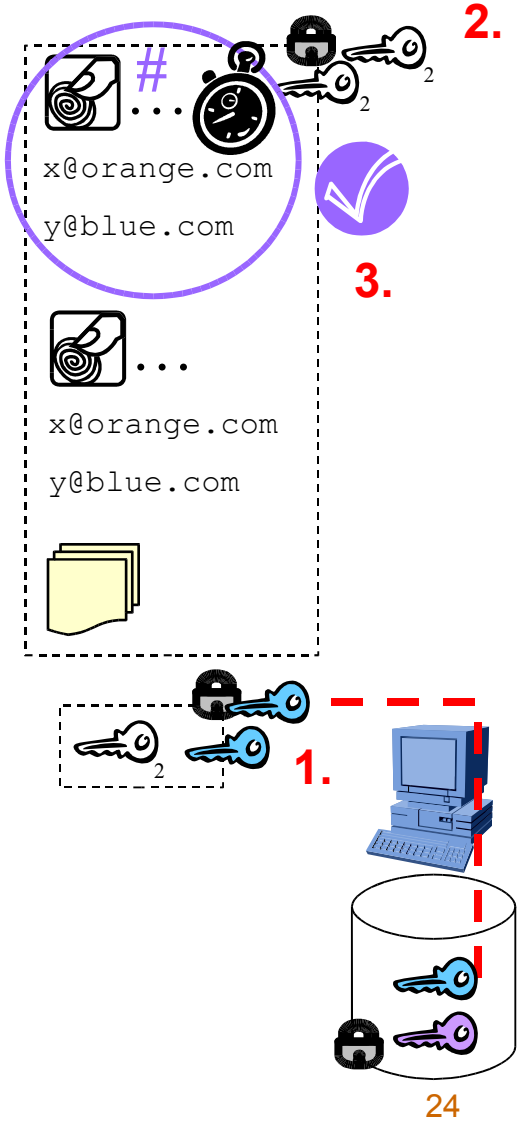
abrica™ dabra

Obvious Security Platform™



1. The Receiver uses their key (Blue) to decrypt the session key (White).
2. With the session key, the Receiver decrypts the payload.
3. The signed content is verified as having come from the Notary Service. The content from Orange is re-hashed by Blue to confirm it matches the signed hash(es).

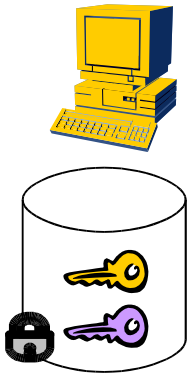




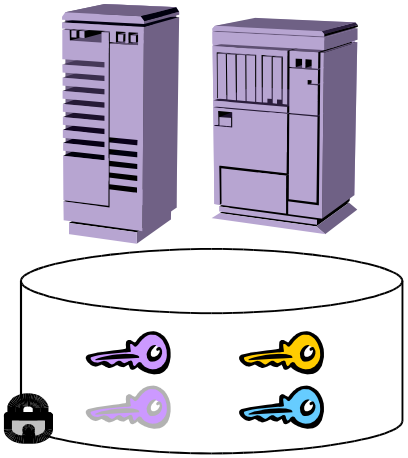
How Does it Work?

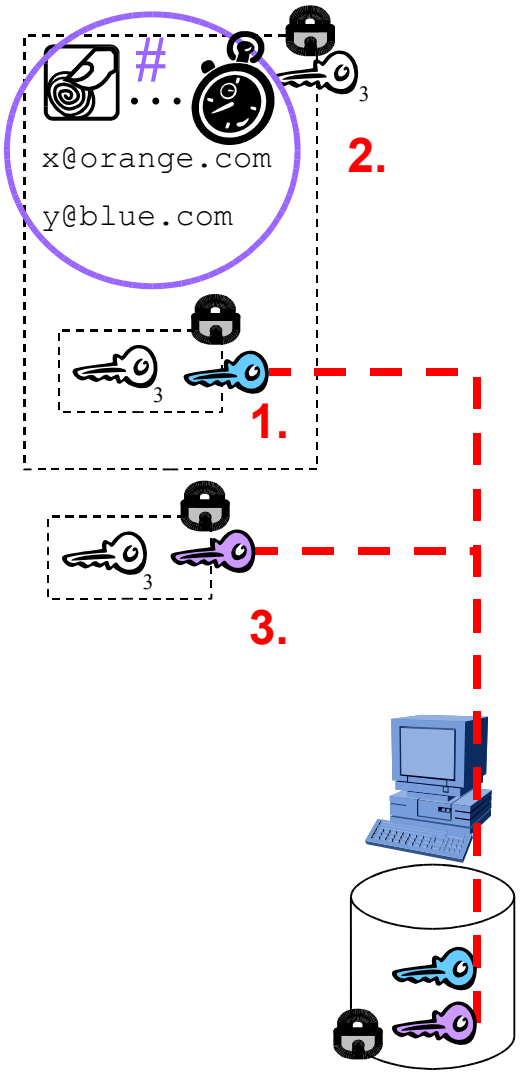
abrica™ dabra

Obvious Security Platform™



1. The Receiver generates a 3rd session key (White), and encrypts it with their Blue key.
2. The entire payload is encrypted with the 3rd session key.
3. The session key is encrypted with the Notary Service public PKI key (dark purple)

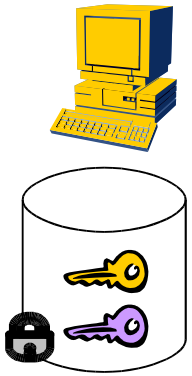




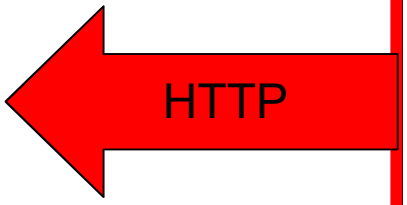
How Does it Work?

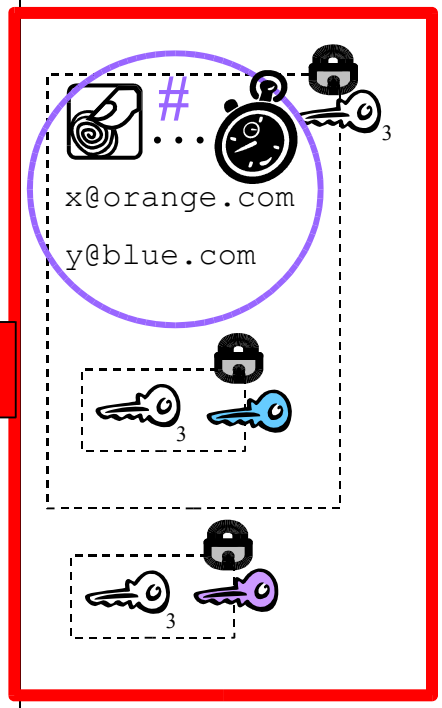
abrica™ dabra

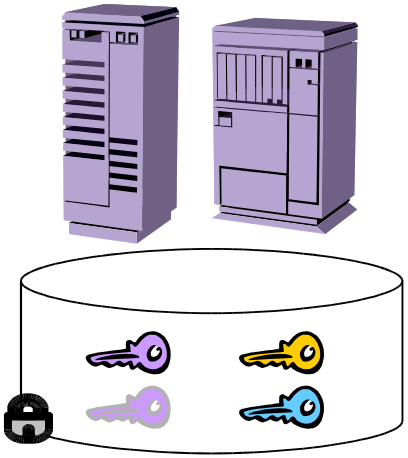
Obvious Security Platform™

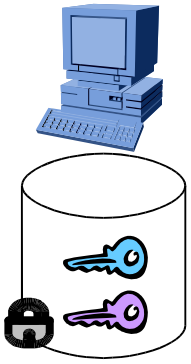


The entire payload is posted to the Notary Service using HTTP.





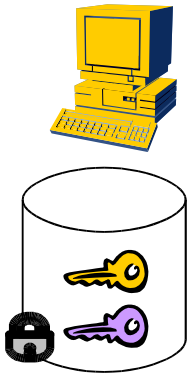




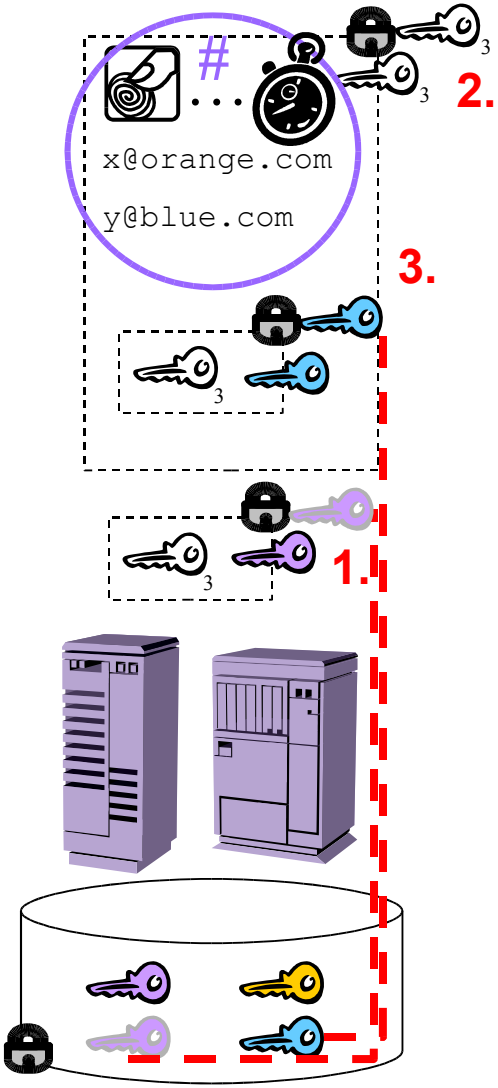
How Does it Work?

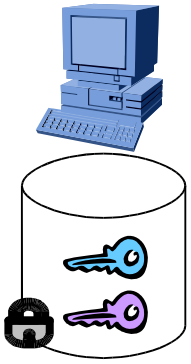
abrica™ dabra

Obvious Security Platform™



1. At the Notary Service, the private PKI key (light purple) is used to decrypt the session key (White).
2. The session key is used to decrypt the payload.
3. Based on the signed content, the initiator of the transmission (Blue) is determined and authenticated by using the Blue key to decrypt the session key.

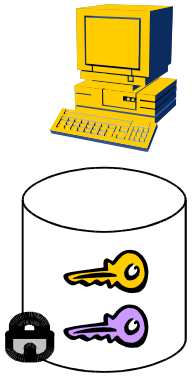


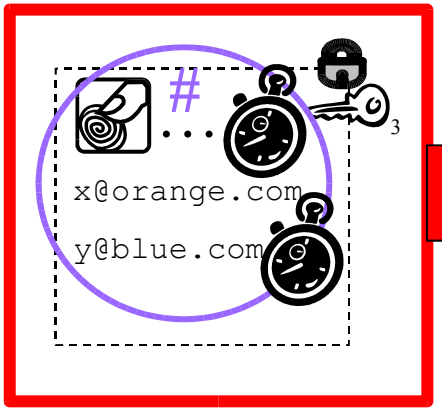


How Does it Work?

abrica™ dabra

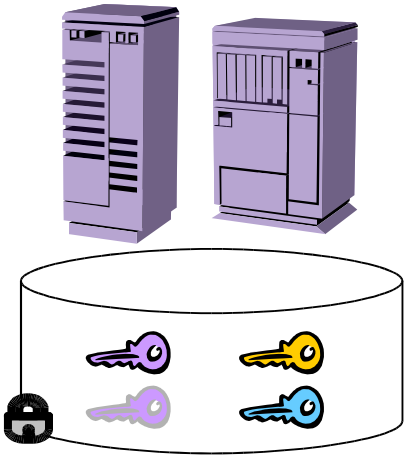
Obvious Security Platform™

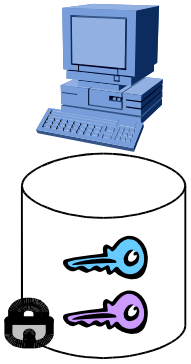




HTTP Reply

1. A second notarized timestamp is added to the signed content, indicating the time of the receipt – and decrypting – of the transmission from Orange to Blue.
2. This signed content is encrypted with the session key and returned to Blue inside the HTTP reply.
3. Since Blue saved the session key, it can decrypt the reply.

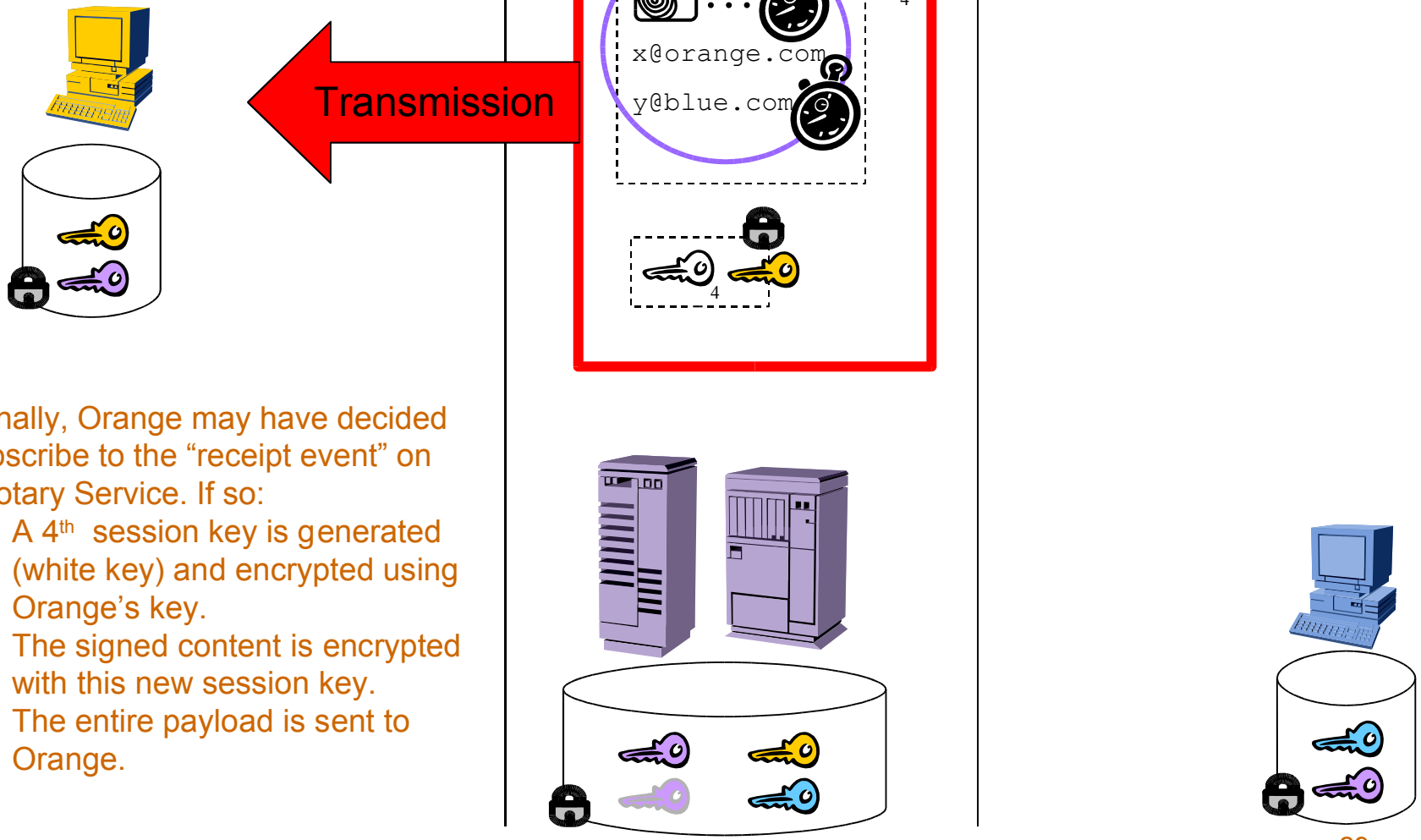




How Does it Work?

abrica™ dabra

Obvious Security Platform™



Optionally, Orange may have decided to subscribe to the “receipt event” on the Notary Service. If so:

1. A 4th session key is generated (white key) and encrypted using Orange’s key.
2. The signed content is encrypted with this new session key.
3. The entire payload is sent to Orange.

Obvious Security Platform™

abrica™ dabra
Obvious Security Platform™

- Obvious' unique, patent-pending security infrastructure:
  - **Authenticates** sender and receiver
  - **Encrypts** all transmitted content, regardless of the transport protocol used
  - **Works with or without firewalls** or other border security technologies
  - Generates **non-repudiation audit trail** of all payload content
  - **Doesn't require PKI** certificates at each node
  - Encrypts/Decrypts payload content **1000x faster** than using PKI keys
  - Is able to send and authenticate in a **single transmission** (PKI requires 2 transmissions)