Applied Digital Receipt Solutions for e-Commerce

Integrating Digital Receipt Solutions into e-Commerce Transactions

ValiCert

Applied Digital Receipt Solutions for e-Commerce

Overview

For companies that conduct business online, the ability to prove that transactions took place is of paramount concern. Without legal-grade proof of e-Transactions, a company's business partners and customers will refuse to make critical business purchases online.

To provide proof for e-Transactions, companies in the B2B, financial, and healthcare industries continue to rely on paper-based evidence with handwritten signatures. Paper-based systems for managing proof, however, lengthen the transaction life cycle, increase the costs of managing and maintaining evidence, and increase the likelihood of costly errors.

ValiCert's Digital Receipt Solutions provide legal-grade proof management that eliminates the need for traditional paper-based evidence. Digital Receipt Solutions offer non-repudiation for e-Transactions by capturing transaction specific information, and safeguarding these transaction details in a tamper-evident digital vault.

Digital Receipt Solutions allow transactions and documents to be digitally signed, time-stamped, verified and audited in a standardized way. Digital Receipt Solutions can reduce the legal liability associated with electronic commerce and dramatically increase the efficiency of tracking e-Transactions for auditing purposes.

This paper describes how to use ValiCert's Digital Receipt Solutions to manage proof for Internet and wireless e-Transactions.

From EDI to e-Commerce

Business-to-business (B2B) electronic commerce evolved from standard Electronic Data Interchange (EDI), which reduced risk by requiring legal trading partner agreements and the security of private networks.

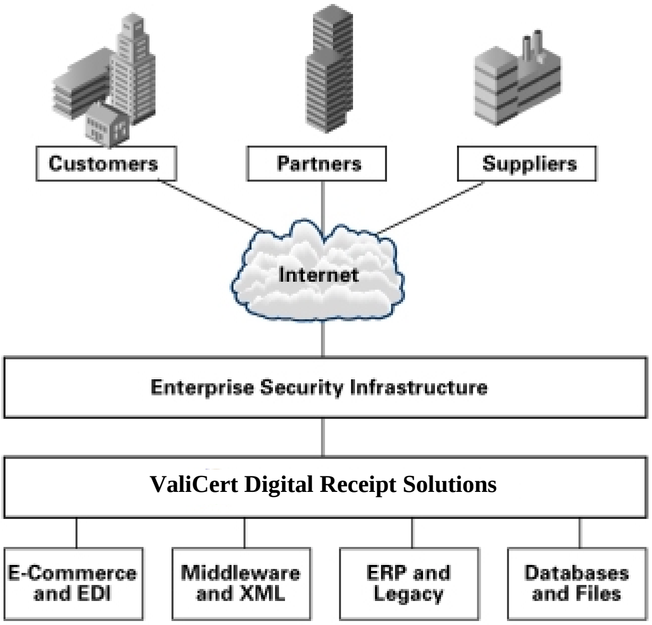
EDI can support procurement efficiencies, enable savings by automating tasks, increase accessibility of information among vendors, and provide stronger links to customers, partners, and suppliers. But the scope of EDI has always been limited—intentionally—to ensure controlled activity within a closed-door environment. Because of the heavy overhead associated with the EDI infrastructure, many small, medium, and even large businesses have been shut out.

As business-to-business electronic commerce explodes onto the Internet, the old protections of private network with centralized mailboxes and audit no longer exist. Furthermore, daunting new risks appear because more money is at stake as the circle of electronic trading partners expands. Transactions themselves are growing more complicated and inter-related as businesses become dependent on their trading partners' enterprise data.

Non-Repudiation and binding electronic evidence

To date, Internet security has focused on authentication, access control, and data privacy. While these are critical components in a secure electronic commerce system, they fall short of ensuring that critical transactions and communications can be relied upon for next generation electronic business. For the global economy to become truly reliant on extranets and electronic commerce, communications and transactions over the Internet must become binding and provable. Transaction integrity and authenticity must be verifiable, even for complex transactions between numerous trading partners. Digital Receipt Solutions provide this software and services infrastructure.

Figure 1. ValiCert's Digital Receipt Solutions integrate diverse e-commerce applications with unforgeable, auditable and verifiable XML receipts



Managing e-Transactions

As e-Commerce continues to explode, businesses and consumers alike will be faced with the challenge of managing a deluge of electronic transaction data. Businesses will need to understand and track online bills, purchases and financial transactions, and will be barraged with transactions from a variety of information systems as more corporate functions such as human resources, purchasing and finance migrate to e-commerce applications. The volume and variety of these transactions require a universal format so that they can be collated, reconciled and understood. A standard transaction record enables internal and external auditors to reconcile e-commerce transactions and to rely on the integrity and accuracy of these transactions.

Extensibility of XML

ValiCert's Digital Receipt Solutions harness the extensibility of XML, which enables them to adapt to any environment without compromising the integrity of the specification. XML is the ideal platform for managing transaction data as it is emerging as the de facto standard for e-commerce applications and middleware.

Collation and reconciliation

Like paper-based transactions, e-Commerce transactions typically have multiple steps and source documents for each step. Gathering and comparing this information is critical for verification and reconciliation. Paper is the standard in the physical world that enables the details of each step to be compared. In e-Commerce, where many dissimilar applications may contribute to the transaction flow, a standard for transaction data is essential for collation and reconciliation.

Even the simplest of business-to-business e-commerce work flows may have several key exchanges that might later be required to assemble the flow of the exchange that occurred between two or more parties on the Internet. Digital Receipt Solutions track and protect key audit points during these vital electronic business transactions.

Real-time assurance

A critical component of binding global electronic commerce is the implementation of broad-based Digital Receipt Solutions for insuring, verifying, notarizing and auditing transactions and communications over the Internet. This infrastructure allows accounting firms, banks, insurance companies and government regulatory agencies to become directly involved in the electronic economy by providing real-time assurance services. These services will make the Internet an appropriate environment for the trillions of dollars of business commerce that is to come.

Digital Receipt Solutions Enable Non-Repudiation

Non-repudiation is the ability to prove to a third party, after the fact, that a message or transaction did in fact occur between two parties. Digital Receipt Solutions provide non-repudiation through the use of digital certificates, online transaction witnessing, and unforgeable archiving. Non-repudiation is also used to prevent illegitimate breaches to contractual agreements. Digital Receipt Solutions combined with digital certificates turn non-repudiation into reality.

ValiCert's Digital Receipt Solutions produce Transaction Confirmations which are XML documents that validate transactions or communications that occur between two parties. Digital Receipt Solutions ensure the authenticity of the time-stamp, digital signatures, and transaction details, and can be used to provide evidence to a third-party should a dispute arise and documented proof become necessary.

Digital Receipt Solutions provide a standards-based system for managing proof that enables binding e-Transactions. By placing application-specific transaction detail within a non-repudiable envelope, Digital Receipt Solutions effectively achieve the following:

- Evidence Creation
- Evidence Storage
- Evidence Access
- Evidence Verification

Digital Receipt Solutions meet the requirements of the fundamental types of non-repudiation: origin and delivery.

Non-repudiation of origin

Non-repudiation of origin protects the recipient of a transaction by confirming the identity of the originator. It ensures that the following questions can be answered without dispute:

- Who initiated this transaction?
- What was transacted?
- When was the transaction completed?
- Was the transaction tampered with during transmission?

Non-repudiation of delivery

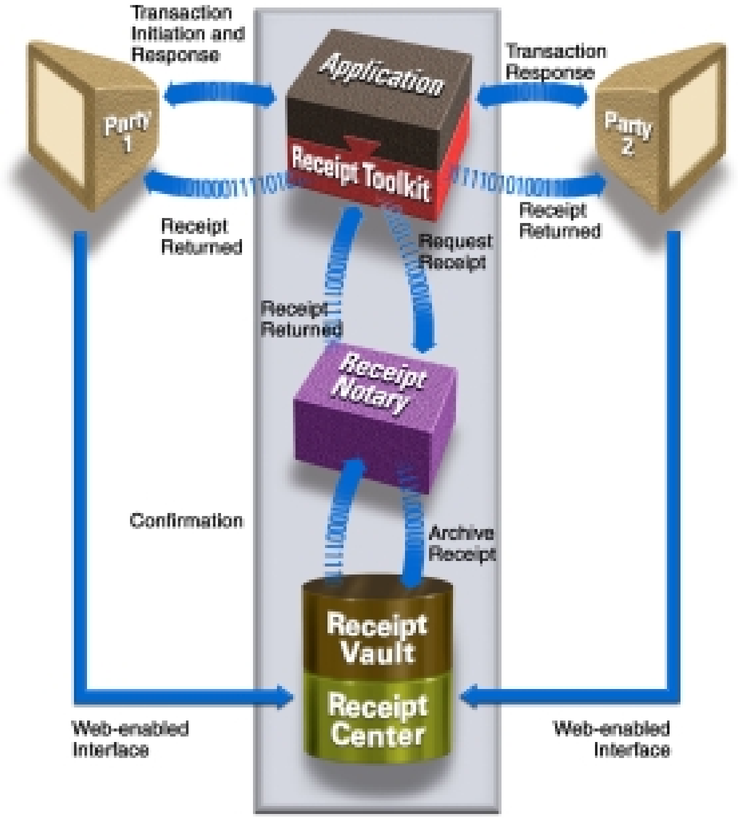
Non-repudiation of delivery protects the sender of a communication by guaranteeing essentially the same elements as the non-repudiation of origin. It ensures that the following questions can also be answered without dispute:

- Was my transaction initiated?
- What was transacted?
- When was the transaction completed?
- Was the transaction tampered with during transmission?

Components of ValiCert's Digital Receipt Solutions

Digital Receipt Solutions have three essential components: Receipt Notary, Receipt Vault and Receipt Center. Receipt Notary produces Transaction Confirmations, and delivers them to the Receipt Vault. The Receipt Vault provides centralized storage, reconciliation and reporting of transaction records and confirmations. The Receipt Center is the web-based application that allows users to search, summarize and view Transaction Confirmations from their desktop and browser.

Figure 1. Digital Receipt Solutions Architecture



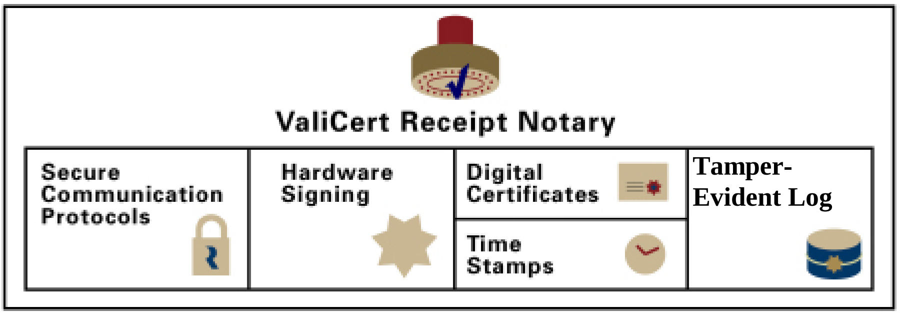
Receipt Notary

ValiCert’s Receipt Notary is a scalable server, which produces XML-based Transaction Confirmations that capture various elements of a transaction, including the parties involved and the time of a transaction. The server also delivers the Transaction Confirmations to a centralized storage repository, the Receipt Vault.

The Receipt Notary manages the process of generating all the evidence required to support non-repudiation of both origin and delivery. It uses the private keys of all parties involved to generate tamper-evident Transaction Confirmations that encapsulate all of the transaction evidence. This is accomplished when Digital Receipt Solutions interface with trusted third-parties such as certificate authorities and time-stamp servers to obtain objective, bulletproof information. The information is then forwarded to the involved parties and optionally stored or forwarded to a Receipt Vault should it be required for later use.

Receipt Notaries can be interfaced with e-mail servers, Web applications, payment gateways, file transfer systems, document management systems, middleware, EDI servers and other transaction processing systems to provide a comprehensive solution.

Figure 2. The Receipt Notary



Leveraging Internet protocols, the Receipt Notary can generate cryptographically hardened transaction confirmation documents. Additionally, it delivers them securely, and tracks the receipt of such documents.

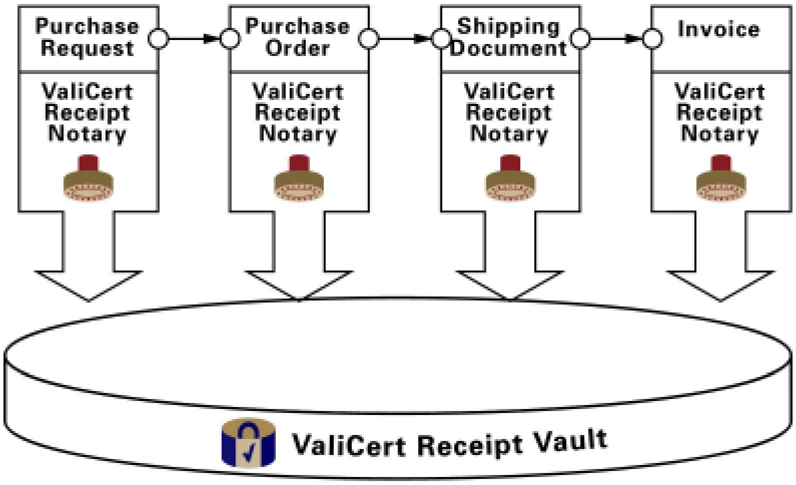
The Receipt Notary provides a uniform format for tracking this data from a wide variety of applications that do not necessarily share data formats. It generates digital signatures and time-stamps to provide data integrity, non-repudiation of origin and time on the tracking data. It generates extensible XML based Transaction Confirmations to record transaction-tracking data.

Receipt Notaries are responsible for creating time-stamps on receipts and for digitally signing those receipts. They can access third-party services for digital notarization, which provides an independent signature, archive and time verification for a receipt.

The Receipt Notary generates tamper-evident logs to detect tampering of tracking data such as deletion or alteration of records. This virtually eliminates risk of fraud or tampering which is usually undetectable at the site where it is generated.

Digital signature acceleration is achieved through dedicated hardware devices, which increase the speed of the generation of Transaction Confirmations.

Figure 3. Receipt Notaries at multiple points of a transaction workflow



Receipt Notaries may be placed at multiple points in the e-Transaction flow. Different events in a transaction may be captured for transaction verification. These events may take place on the private network, over the Internet or at a Commerce Service Provider.

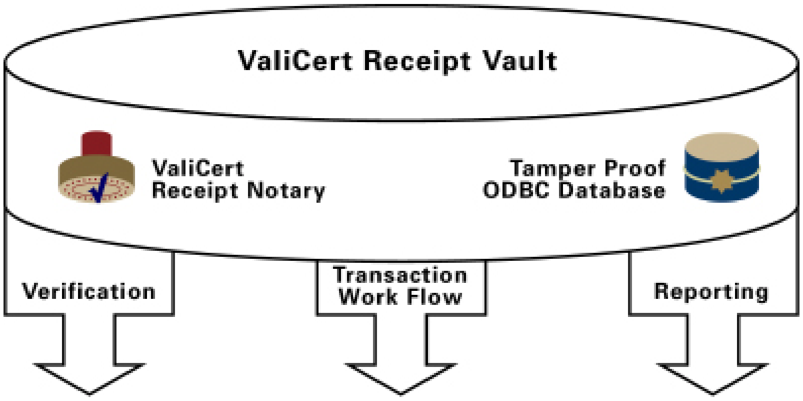
Receipt Vault

ValiCert's Receipt Vault is a high performance server for collating, reconciling, storing, analyzing, querying and validating Digital Receipts. Receipt Vault stores receipts in a database, and has the ability to detect tampering.

Receipt Vault features a Web-based user-interface for tracking, searching and reporting transactions. The system is accessed according to user account permissions. Unforgeable transaction logs and off-site archiving of transactions ensure that data cannot be destroyed or altered without detection.

ValiCert's Receipt Vault is built on industry leading Oracle RDBMS platform. It supports database replication and offline archiving for reliability and high performance.

Figure 4. ValiCert Receipt Vault securely stores and automatically reconciles transactions



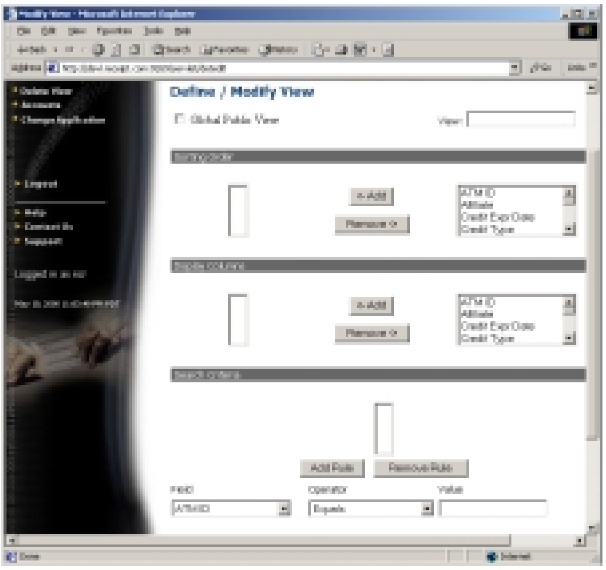
The Receipt Vault stores the Transaction Confirmations in an Oracle relational database for scalability and reliability. The use of a relational database increases the manageability of the tracking data and provides data and query capabilities to generate powerful tracking reports. The Receipt Vault verifies digital signatures on receipts to verify data integrity and non-repudiation of origin of the tracking data, significantly reducing the risk of fraud and tampering of receipts and documents en-route from the Receipt Notary or to the Receipt Vault.

Receipt Center

ValiCert's Receipt Center is an easy-to-use client application that allows end-users to manage secure Transaction Confirmations for commerce transactions from their desktop. The Receipt Center allows the end users to browse and sort Transaction Confirmations. The Receipt Center uses a standard web interface that is familiar to the millions of Windows desktop users worldwide.

The Receipt Center interface allows reports to be created and run interactively. Receipt Center authorization can be structured to allow customers to see only their receipts, merchants to see all their receipts, and operators or auditors to see all receipts in the system. This highly configurable access control makes Receipt Center an ideal application for data mining and reporting.

Figure 6. Receipt Center features customizable reports with a Web interface



ValiCert Trusted Services

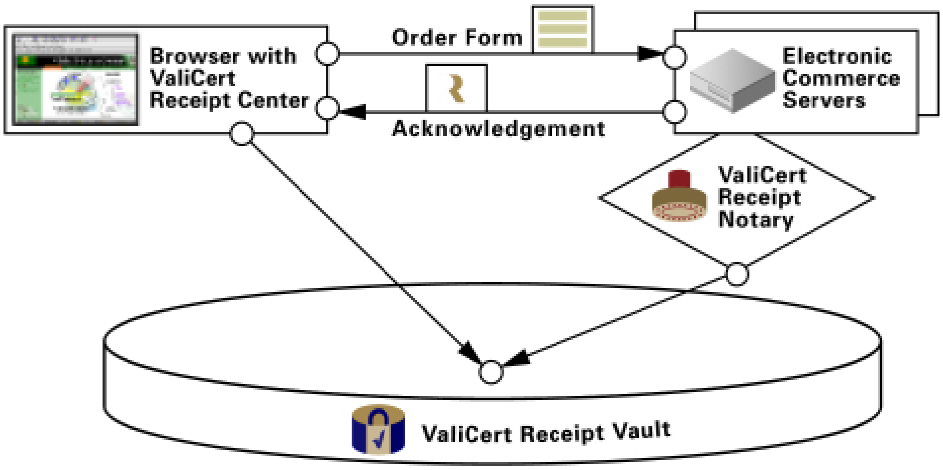
ValiCert provides outsourced Receipt Services from its secure Data Center. ValiCert offers a full spectrum of services for corporations and financial institutions:

- Receipt archiving and transaction reporting
- Secure document delivery and archiving
- Time verification services
- Receipt witnessing
- Trust reports

Managing e-Commerce transaction flows

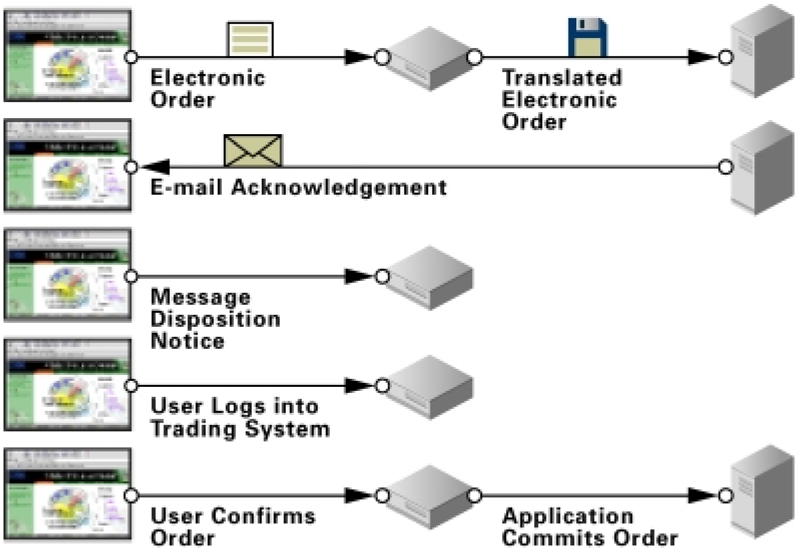
Only a short while ago, Internet commerce was much simpler. A consumer would order products with web forms and credit cards. Large credit agencies such as Visa and MasterCard accepted the risk, creating a worry-free transaction for the consumer below. However, 50% of VISA’s complaints are related to Internet commerce, which is only 2% of its revenue, thus demonstrating the need for binding electronic evidence. Digital Receipt Solutions create and secure transaction histories, thus minimizing the risk for all parties.

Figure 7. An example of e-commerce using Digital Receipt Solutions



ValiCert's Digital Receipt Solutions overlay existing enterprise applications and electronic commerce servers. Transaction Confirmations are triggered by selected events to provide an audit trail of key exchanges by either internal systems or trading partner systems.

Figure 8. Transaction Confirmations monitor key e-Commerce transaction points

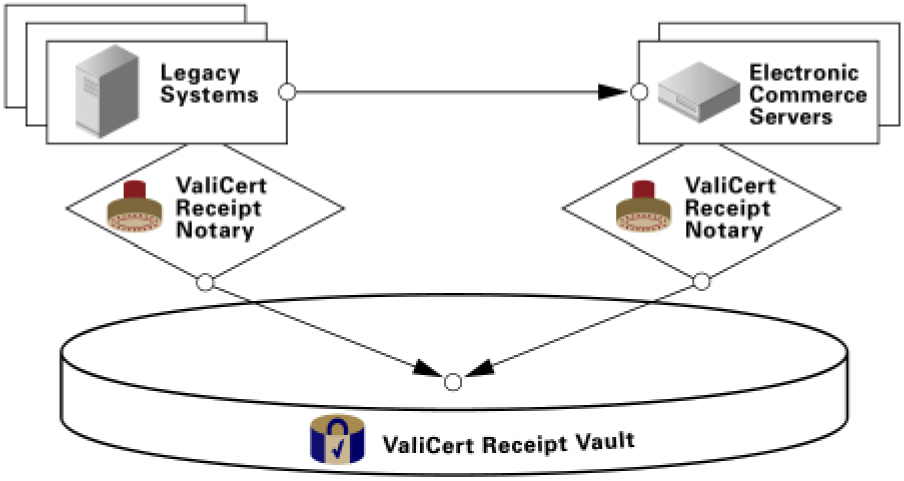

Electronic Order
Translated Electronic Order
E-mail Acknowledgement
Message Disposition Notice
User Logs into Trading System
User Confirms Order
Application Commits Order

Digital Receipt Solutions allow diverse information systems separated by corporate boundaries to create an authentic trail of digital evidence that can be analyzed and compared for completeness and discrepancies.

Legacy electronic commerce integration

Large investments have already been made in EDI, Web Commerce, and Enterprise Resource Planning (ERP) applications. Digital Receipt Solutions have a distributed architecture that is ideally suited to provide a common tracking infrastructure for these disparate systems. The Receipt Notary integrates easily with existing e-Commerce and extranet applications. It is designed to create a trusted commerce system out of existing e-commerce servers.

Figure 9. Digital Receipt Solutions centralize and standardize transactions from a variety of e-Commerce sources.



Extensible XML-based Transaction Confirmations

A Transaction Confirmation is a standard XML document, which captures the essential data of network events or e-commerce transactions. A Transaction Confirmation is defined by one or more Data Type Definitions (DTD), which are based on the Digital Receipt DTD. Transaction Confirmations create a potent e-Commerce infrastructure upon which binding Internet commerce can be conducted, because it not only creates strong electronic evidences but it also supports real time assurance.

Transaction Confirmations are comprised of four key sections <BaseReceipt>, <Signatures>, <Certificates> and <Endorsements> all of which are highly extensible.   The <BaseReceipt> section contains the required fields of the receipt. The <Signatures>, <Certificates> and <Endorsements> sections are optional but provide greater levels of non-repudiation.

The <BaseReceipt> section contains the only required signature, that of the issuer. It also contains links to related Transaction Confirmations to assist in the collation of receipts at a later point in time. Finally, the <BaseReceipt> encapsulates the entire transaction within the XML Document.

Figure 10. Transaction Confirmation Format Overview

```
<?xml version="1.0" ?>
- <Receipt>
        - <BaseReceipt>
                - <Issuance>
                        + <Issuer >
                        + <Timestamp>
                        + <RelatedReceipts>
                </Issuance>
                + <Recipients>
                + <Content >
        </BaseReceipt>
        + <Signatures>
        + <Certificates>
        + <Endorsements>
</Receipt>
```

Endorsements provide links with real-time assurance providers such as notary, audit and archival services.

Standards-based digital signing

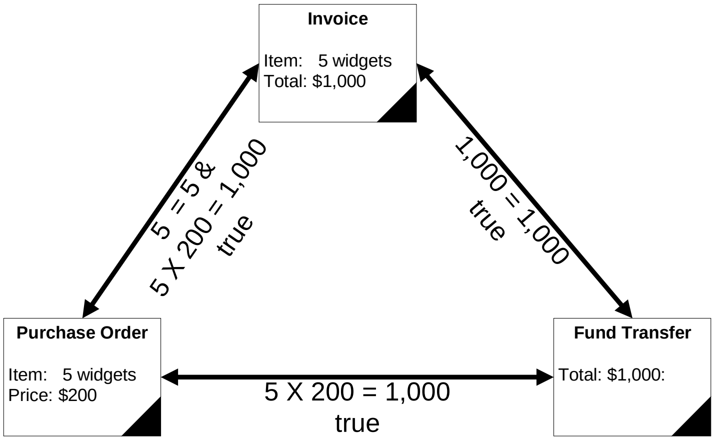
ValiCert is driving the standards for digital signing of XML documents through the IETF and is applying them with Digital Receipt Solutions. Transaction Confirmations leverage pervasive Internet standards such as LDAP directories, X.509 certificates and SSL browsers to capture key transaction data and evidence.

Collation and Reconciliation with Digital Receipt Solutions

The power of Digital Receipt Solutions is demonstrated by the ability to collate and reconcile complex transactions. The Transaction Workflow Engine defines the reconciliation rules; it defines the events to be tracked and how they are related. It also explicitly states which fields should be examined for completeness and accuracy.

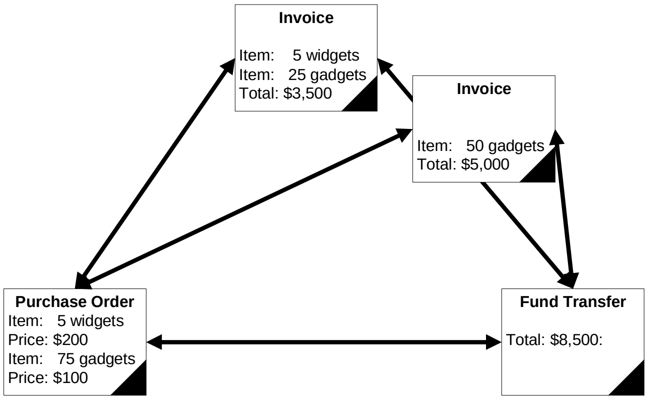
For instance, consider a simple purchasing example that requires one Purchase Order, one Invoice and one Fund Transfer. In this example, the number of items ordered on the Purchase Orders should be the same as the number of items on the invoice. The total amount of the Purchase Order should match the total amount of the funds transferred. The transaction is considered reconciled when all three conditions are true as shown in Figure 11.

Figure 11. A Simple Purchase Transaction Flow



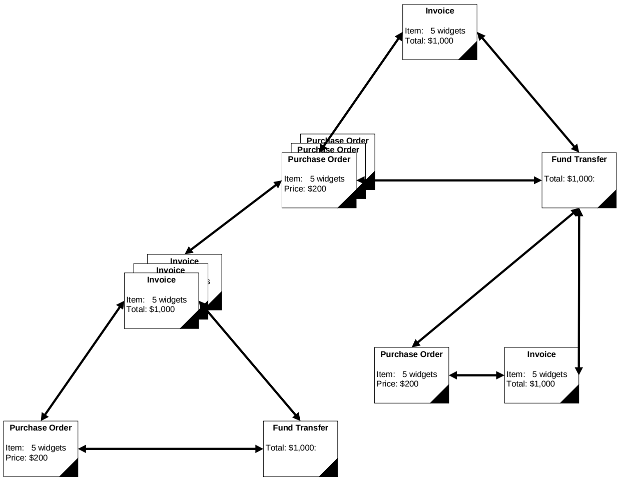
Transactions are rarely so simple in reality. Sometimes all items ordered are not available, they may arrive separately with a different invoice as show in Figure 12 or multiple purchase orders may be invoiced at one time.

Figure 12. A Simple Purchase Transaction Flow with Multiple Invoices



Transactions frequently are more inter-related and often not mutually exclusive. This creates even more complicated scenarios than in Figure 12. For example, one fund transfer may apply to multiple transaction sets or items, or one PO may be separately invoiced and paid.

Figure 13. Inter-related Purchase Transaction Flow



The complexity and risk of business-to-business transactions are compounded as companies race to expand the scope and penetration of their e-Commerce initiatives. Transaction Confirmations create a universal format that allows selected events to be integrated in the transaction workflow with business rules, which define relationships between the audit points.

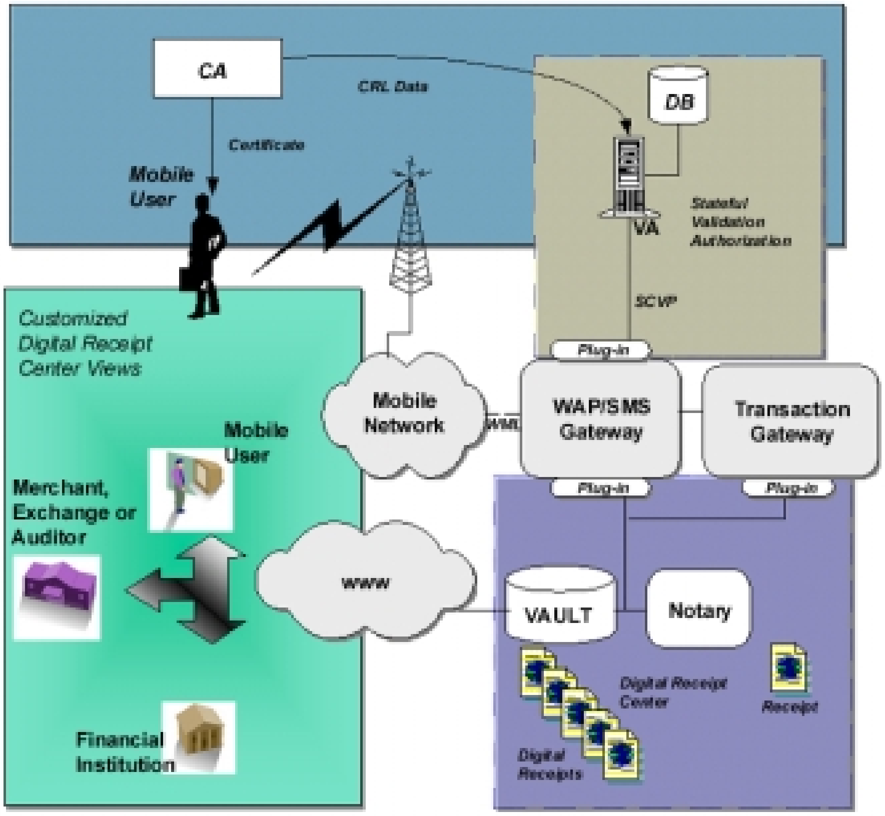
Secure Wireless Transactions

ValiCert's Digital Receipt Solutions are designed to support both Web and wireless applications where security, tracking and proof of transactions are required. The flexible nature of the system allows Digital Receipt Solutions to be integrated into wireless gateways and application servers. Digital Receipt Solutions can support standard or proprietary authentication and cryptographic signing capabilities on mobile devices, and will wrap them in a standard digitally signed XML wrapper. The Receipt Notary can also act as a proxy key and certificate server, signing transactions on behalf of customers.

The Web-based Receipt Center interface allows customers to view their consolidated transaction reports over the Web or on their mobile device. Receipt Center's access control manager allows customers, operators, merchants, financial service providers and auditors or regulatory bodies to view transaction receipts on a highly authenticated and controlled basis.

Receipts can be stored at the mobile operator, the financial service provider, the merchant or a neutral third-party site, such as the ValiCert Digital Receipt Service or a service of a ValiCert Affiliate.

Figure 14. Digital Receipts for m-Commerce



Outsourced Solutions

Because ValiCert's Digital Receipt Solutions are a secure, distributed architecture, all or part of the system can be outsourced. This allows records of digitally signed transactions and documents to be hosted in a neutral third-party data center, providing a level of assurance that data cannot be tampered with. This can be important for meeting regulatory compliance requirements in a variety of industries.

ValiCert's secure Data Center offers customers the utmost in security, reliability and performance for critical outsourced applications. The data center is engineered and operated to "Trusted Third-Party" levels. Operations are audited to ensure compliance with practice statements. This level of care and precision allows liability to be quantified and insured against.

ValiCert and its affiliates operate data centers with the following features:

Physical Security

- Walls are reinforced with Steel Mesh
- Isolated Power source
- Automatic UPS & Generator
- Redundant Leibert HVAC System
- Leak detection & environmental monitors
- Multi-level security enclosures within data center
- Multiple biometric recognition devices controlling access points
- RFI shielding of core services
- Standalone ACME Security System
- Close Circuit TV monitoring – inside & outside

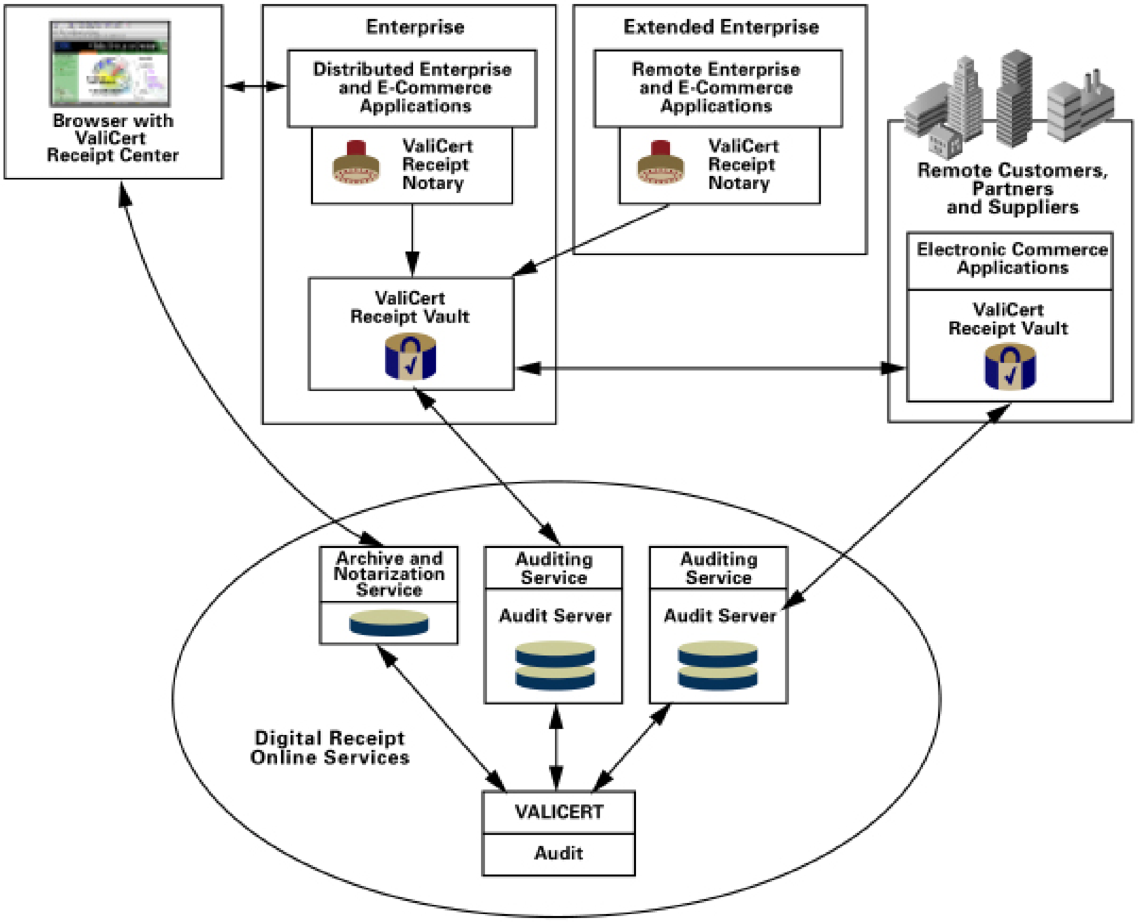
System and Network Features

- Tier 1 ISP vendors
- Fiber and copper local loop POP
- Redundant connections to the internet
- Leading edge switching & router technology
- Gigabit switched backbone – front to backend
- Multiple levels of load balancing via local directors
- Hierarchical layered network security design
- Complete network, systems and database redundancy
- High Availability via Veritas Clustering
- End-to end monitoring and health checks
- Daily systems and data backups (delta)
- Weekly full backups & offsite archiving

Closing the Loop with Real-time Assurance Services

ValiCert's Digital Receipt Solutions provide a potent infrastructure that allows companies, customers and auditors to verify the accuracy and completeness of complex transactions. Transactions that may cross network or corporate boundaries are securely and centrally stored in the Receipt Vault. The server automates verification of events and identities and enables other forms of real-time assurance such as online attestation, notarization and insurance.

Figure 15. Putting it all together



Browser with ValiCert Receipt Center
Enterprise
Distributed Enterprise and E-Commerce Applications
ValiCert Receipt Notary
Extended Enterprise
Remote Enterprise and E-Commerce Applications
ValiCert Receipt Notary
Remote Customers, Partners and Suppliers
Electronic Commerce Applications
ValiCert Receipt Vault
ValiCert Receipt Vault
Archive and Notarization Service
Auditing Service
Audit Server
Auditing Service
Audit Server
Digital Receipt Online Services
VALICERT
Audit

The infrastructure allows internal and external auditors to share selective transaction details with each other.

Third-parties such as auditors and financial institutions can now verify all aspects of a transaction. The identity of the individuals, applications, and companies that witnessed events, and the exact time the transactions occurred, are verifiable by third-parties. Log files alone make auditing these transactions very difficult.

However, archiving Transaction Confirmations in a tamper-evident relational database enables real-time analysis and reporting of audit history.

Verification of Digital Signatures and Time

Both the Receipt Notary and Receipt Vault validate the identities of all parties using digital certificates from any major CA.

Some transactions such as stock trades and online auctions are particularly time sensitive. Trusted time sources can also be used to time-stamp or synchronize electronic commerce server clocks for time sensitive transactions.

Notarization

Online notaries are emerging to fill the space that traditional notaries have filled for centuries in the paper world. Public key and other forms of strong authentication such as biometrics and onetime passwords are now being adopted domestically and internationally for binding signatures. Electronic notaries leverage this technology to offer protection beyond their paper-based predecessors by taking a digital fingerprint of a document and providing real time verification of a document's integrity.

Electronic Audit

ValiCert Digital Receipt Solutions allow internal and external auditors to gather and compare all of the source documents related to a transaction. The Receipt Vault can publish Transaction Confirmations to corporate auditors and enterprises to share information with their audit authorities.

Evidence Retention

Users and corporations have the option of archiving their Transaction Confirmations locally or on a network-hosted service. Either way, the data must be stored in such a way as to prevent tampering or deletion. The perishability of electronic evidence such as Transaction Confirmations is also being address by third-party online services.

Transaction Confirmations can be retained and archived for an indefinite period of time.

Conclusion

ValiCert's Digital Receipt Solutions provide an important component of the e-commerce security puzzle by delivering true non-repudiation. By standardizing electronic evidence, Digital Receipt Solutions enable real-time assurance and reconciliation of electronic commerce transactions. In the same way that Public Key Infrastructure provides a standard for authentication, Digital Receipt Solutions provide a standard for transaction tracking, time-stamping, validation and reconciliation.

About ValiCert

ValiCert is a leading provider of secure E-Transaction infrastructure products and services for conducting business safely over the Internet. ValiCert's validation, transaction assurance and proof offerings provide corporations and e-business exchanges with a certificate- and payment-neutral infrastructure for protecting all phases of the e-Transaction life cycle. ValiCert's products and services are available through its worldwide network of affiliates and partners.

ValiCert has technology and marketing alliances with leading worldwide providers and users of security services and products. The company's customers include Global 2000 organizations in financial services, telecom, healthcare and government sectors. ValiCert is headquartered in Mountain View, California, and is available on the World Wide Web at www.valicert.com.