White Paper

Protecting e-Business Applications and Content

Probix, Inc.
883 N. Shoreline Blvd.
Mountain View, CA 94043

Probix, Inc. reserves the right to revise this description and to make changes to its products and services specifications from time to time without notice.

Probix, Trustee, Content Protection Services, Digital NDA and ePouch are trademarks of Probix, Inc. Other names of products or services mentioned may be trademarks or registered trademarks of their respective owners in various jurisdictions.

Revision History:

2001/1/17	*Version 1.0 RM*
2001/1/26	*Version 1.1 RM*
2002/7/22	*Version 1.2 RM*

Executive Summary

With the phenomenal growth of the Internet, and as the corporate use of the web has exploded, the focus has changed from providing general information to much more specific, highly confidential information. Corporations are realizing the importance of using the Internet to support key business functions. The web is rapidly becoming the primary platform through which corporations collaborate with their suppliers, partners, customers and employees. New web-based technologies are being incorporated into nearly every business function: purchasing and procurement, product development, supply-chain management, demand forecasting, production scheduling and management, manufacturing and logistics, and sales and marketing.

By having a fast and efficient communication and collaboration platform with their business partners, corporations can use the rapid information flow to significantly bring down their cost, reduce inventories and accelerate product development cycle. Yet, for the information to flow freely, they must have complete confidence that their content would remain secure throughout the information's life cycle. Whether the information contains purchasing, sales, forecasting, planning or financial information, confidentiality is always the number one concern. If the information leaks, a company's competitive edge could be adversely affected.

The ability to ensure the safety and confidentiality of the information, coupled with the ability to track the content as it flows through the supply chain and provide detailed audit trial information to the content owner is with no doubt one of the most important enablers of e-business in any industry.

The nature of information security threats has changed as organizations expand their use of the web, shifting their focus from intranet-based applications to extranet-based portals, private e-hubs and B2B exchanges. Therefore, more sensitive information is being made available via the web.

At present, security technologies allow content providers to protect confidential information stored on the corporate web server from being accessed by non-authorized users. This is done though firewalls, authentication and access control systems. The information is also secured as it flows through the Internet, using technologies such as Virtual Private Networks (VPN) and Secured Socket Layer (SSL). However, when the information is delivered to the authorized user, the content provider has no means of controlling what the user does with the confidential information. The user can easily forward the information by email to a third party, print it or copy it digitally.

Probix Trustee™ allows content providers to set usage policies, enforce those policies on the users' workstations and provides the content owner with a detailed audit trail of any operation performed on the protected information.

Leveraging a strong industry trend to outsource security services, such as managed Firewalls and managed VPN, Probix Trustee is delivered as a managed service (on-site or off-site) on a monthly subscription basis or as a software license.

1. Managing Trust in e-Business

1.1 Basic Services

B2B collaborative commerce is expected to become mission-critical for many industries. OEMs and suppliers are migrating paper-based processes in the areas of procurement, supply chain management and product development to the Internet. Yet, along with all the tremendous benefits B2B can bring, there are still many challenges to overcome in many different aspects of the business. There are cultural issues that need to be dealt with, business processes that need to be changed, technological challenges, etc.

One of the most important set of challenges revolves around the concept of 'managing trust'. To conduct business online securely and confidentially, to share confidential information with business partners, there are a series of requirements that need to be satisfied:

- **Authentication** – Buyer and sellers need to be able to reliably establish and verify the identity of their customers and partners.

- **Payment** – Financial transactions need to be executed and verified with the same level of security and confidence as in the traditional, paper-based world. Mechanisms need to exist to validate that transactions actually took place to prevent fraud and resolve potential future disputes.

- **Confidentiality of Content** – To exchange confidential content with their partners, companies need to be able to maintain control over this information at all times and to track it as it gets disseminated through the various supplier tiers.

The first two requirements for authentication, payment and validation are being addressed by companies such as VeriSign that provide a comprehensive set of services that include digital certificates, automated fully secured payments and validation services. VeriSign provides a robust, highly secured public key infrastructure (PKI) and Certificate Authority (CA) system for issuing digital certificates as online credentials

The third requirement for maintaining the confidentiality of the content is addressed by Probix Trustee. As the first content protection service provider, Probix Trustee creates a secure collaborative environment that enables corporations to freely share intellectual assets with customers, partners and employees. Trustee provides protection against misuse and tampering, and allows content owners to remain in control of their digital properties at all times.

1.2 The Challenge of Maintaining Control Over Confidential Content

Successfully managing and securing corporate intellectual property has become a more complex challenge as corporate use of the web has matured. Organizations are establishing secured extranets so they can collaborate more effectively with their business partners. As corporations are making more sensitive information available to access from outside the corporate firewall, the nature of information security threats is changing as well. In this section, we will examine the traditional information security technologies and describe how Probix Trustee complements the existing security infrastructure and expands the security envelope to protect highly confidential information even after it has been delivered to an authorized user.

Most information security technologies can be divided into the following three categories:

- **Authentication** – A system used to identify the users attempting to access confidential content. Numerous authentication technologies are being used including, user name and password, digital certificates, smart cards, tokens, etc.

- **Access Control** – Systems designed to allow authorized users to access confidential information. Once the user credentials were established using the *authentication* system, it's the responsibility of the *access control* system to allow access to only those users that were authorized. Firewalls, which are typically used to prevent unauthorized Internet users from accessing private networks connected to the Internet, are *access control* devices.

- **Privacy** – Various technologies and systems designed to maintain the privacy of the information as it is transferred through the network. For example, a Virtual Private Network (VPN) is a technology that creates a secured network between multiple sites, using the public Internet to connect them. A VPN is designed to maintain the privacy of the information as it is transferred through the non-secured Internet. Secured Socket Layer (SSL), typically used to secure transactions in which confidential information (such as credit card information) is exchanged, is another example of such technology.

These technologies provide the following security coverage:

- Secure the web server content from being accessed by non-authorized users
- Ensure that authorized users can access the information
- Secure the communication channel as the information is delivered over the Internet to authorized users.

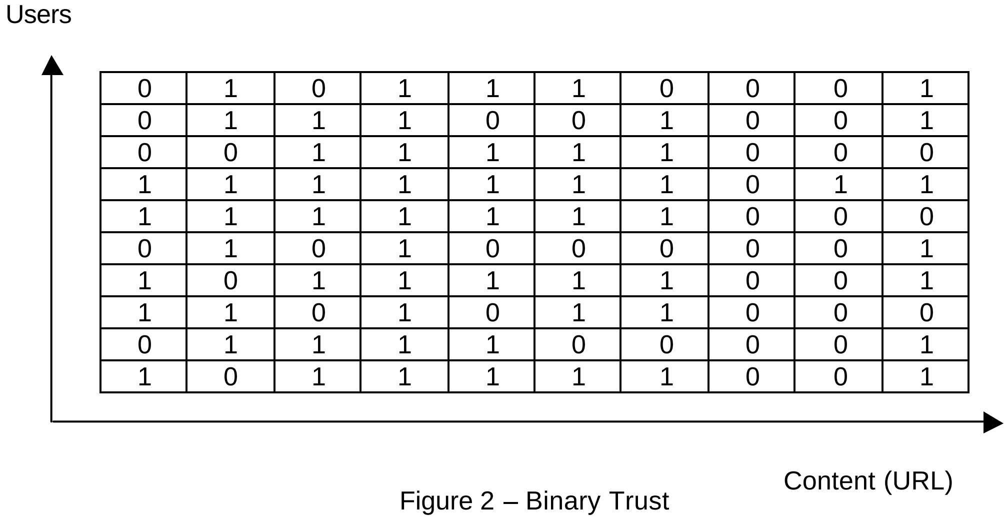
Yet, once the content is delivered to the 'authorized user' – it is no longer secure. Once the user receives the content, the provider of that content has no control over what the user can do with it. He/she can forward it by email to a third-party, print it, copy and paste the information digitally as part of a proposal to a competitor, etc.

1.3 Granularity of Trust

At present, web-based access control technologies handle trust as a binary concept. 'Trusted' users are given access permissions to information they are authorized to access. Once they receive the information, they are free to use it any way they choose to.

Within an enterprise, collaborative platforms such as Lotus Notes and Microsoft Exchange, offer a more refined set of security policies that control not just who accessed the information but who has the permission to modify it. Yet, the focus is on the collaborative aspect of multiple users creating, sharing and modifying documents. The same core problem still exists – there is no control of the information after it has been delivered to an authorized user.

To illustrate this point, Figure 3 shows a two dimensional matrix. The X-axis represents the content, or the information being accessed. The Y-axis represents the users that need to have access to this information. Zero ('0') represents no access, and one ('1') represents permission to access the information.


Users
Content (URL)

0	1	0	1	1	1	0	0	0	1
0	1	1	1	0	0	1	0	0	1
0	0	1	1	1	1	1	0	0	0
1	1	1	1	1	1	1	0	1	1
1	1	1	1	1	1	1	0	0	0
0	1	0	1	0	0	0	0	0	1
1	0	1	1	1	1	1	0	0	1
1	1	0	1	0	1	1	0	0	0
0	1	1	1	1	0	0	0	0	1
1	0	1	1	1	1	1	0	0	1

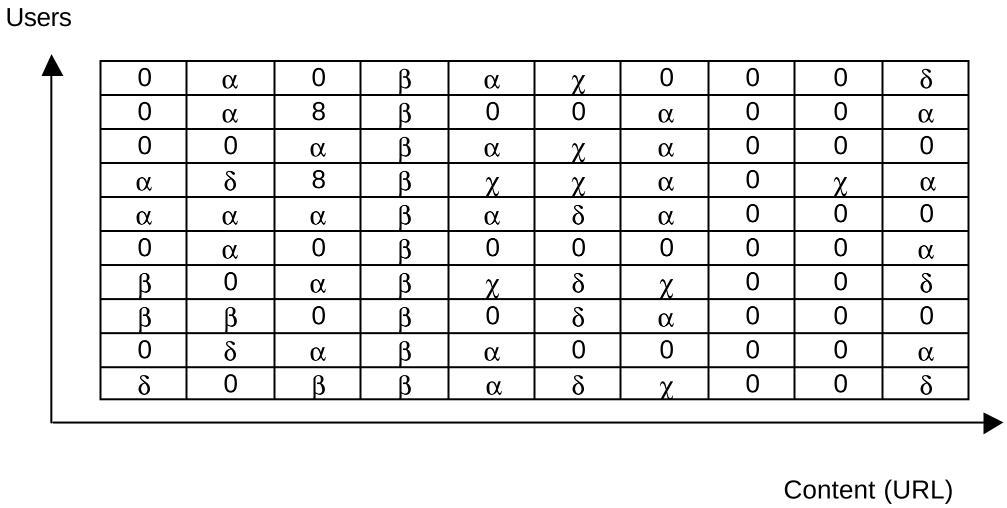
Figure 2 – Binary Trust

This is a simplistic approach to information security, driven by technology. The business reality, however, is different. In the 'paper-world' where Non Disclosure Agreements (NDA) are often used, not all business partners or suppliers are treated the same way. Some partners may be trusted more than others and may therefore be less restricted in the way they use the information. Others may have more restrictions, either because trust has not been fully established yet or because there is no business need to justify risking loss of intellectual property. Frequently, information is provided on a need-to-know basis based on specific business requirements.

In the off-line business world, when businesses and legal entities have a need to exchange confidential information, most often the processes are paper-driven, face-to-face contacts, with clear rules of engagement, and a clear split of value-added functions. This has been traditionally accomplished by having strict hierarchies and by minimizing external and internal interfaces.

Probix Trustee brings the concepts of 'Granularity of Trust' and a 'Digital-NDA' to the on-line world. 'Trust' is no longer binary. A user who has access rights to the information may not have permission, for example, to print it or save it on their workstation. Probix Trustee allows content owners to establish content policies for their partners and suppliers based on a need-to-use basis, thus protecting the information against misuse.

To illustrate content protection policies, we'll use the same matrix as in Figure 2, and replace the one's with an integer value (α, β, χ, and δ) that represents a set of permissions (policy) granted to an individual user or group of users. The zeros, of course have not changed, since they represent those users who do not have access permissions to the information.



0	α	0	β	α	χ	0	0	0	δ
0	α	8	β	0	0	α	0	0	α
0	0	α	β	α	χ	α	0	0	0
α	δ	8	β	χ	χ	α	0	χ	α
α	α	α	β	α	δ	α	0	0	0
0	α	0	β	0	0	0	0	0	α
β	0	α	β	χ	δ	χ	0	0	δ
β	β	0	β	0	δ	α	0	0	0
0	δ	α	β	α	0	0	0	0	α
δ	0	β	β	α	δ	χ	0	0	δ

Figure 3 – Granular Trust

2. Introducing Probix

2.1 Overview

Probix Trustee allows content providers to set content usage policies, enforce those policies on the users' workstations and provide the content owner with a detailed audit trail of any operations performed on the protected content.

Probix Trustee can be used to protect content on any of the following platforms:

- Corporate web sites
- Corporate portals (for both intranet and extranet users)
- Private or public B2B exchanges

The solution allows web administrators to assign content usage policies to individuals or groups of users. It enforces those policies when the content is delivered to users' workstations and reports to the content owner a comprehensive audit trail of when and to whom the content was distributed and the operations performed by each user (such as saving locally, printing, e-mailing, etc.)

2.2 Policy Setting

The content administrator is responsible for setting policies on behalf of the content owner. The setting of policies is accomplished using a Probix-provided Web interface, which allows policies to be associated with individual digital objects, or with sets of such objects. Policies can be established for individual users, or for groups of users.

This tool allows the content administrator to create and maintain multiple policy profiles. Each profile is composed of three components:

- **Content** – This may be a set of directories, individual documents or web pages that need to be protected. The utility provides a view of the web server's content and allows the administrator to tag each element that requires protection. Probix Trustee™supports many different file formats such as: HTML, PDF, JPEG, GIF as well as Microsoft Office documents such as Word, Excel, PowerPoint, etc. It can also be applied to dynamic content such as HTML files that are dynamically created through the use of Active Server Pages (ASP), CGI scripts, etc.

- **Users** – The content protection policy can be set globally for all users accessing the web site or separately for each user or a group of users that have been granted access to the information through the access control system. Probix Trustee utilizes LDAP (Lightweight Directory Access Protocol) to access the user directory and integrates with numerous access control systems.

- **Operations** – A set of operations the user has permission to perform on the protected information. Restricted operations may include:

    - Actions such as: save, print, copy, forward (e-mail) etc.
    - Temporal restrictions. Policies can also be set to allow operations to be performed on the information for a specific period of time. For example: users may be allowed to view particular information for only three days or until a certain date.

- Cardinality of access - Policies can also be set to allow an action to be performed only a limited number of times or in a certain order.

To simplify the configuration process some actions may be grouped together to form a security profile (high, medium, low and custom level).

2.3 Policy Enforcement

When a user attempts to access protected information, he/she gets authenticated, and based on the access control policies, is given access to the information. If the content is ‘tagged’ as being protected, the request will then be re-directed to a Probix server. If the protected content is not currently cached on the Probix Trustee, a copy of it is requested from the owner’s Web server. This request is made *via* a VPN or by a secure link provided as part of Probix Trustee.

The Probix server compresses and encrypts the content, and ‘wraps’ it with an encrypted package containing the policy information and Java mobile code. This encrypted package, referred to as the ‘ePouch’, is then delivered to the client, where the mobile code is executed.

The mobile code then requests the data encryption key from the Probix server, unwraps the content and displays it. If the policies associated with the information do not allow printing or saving to local disk for example, those browser functions are temporarily disabled. The user is unable to activate any of the actions that are prohibited by the policy.

2.4 Audit Trail

Probix Trustee allows content owners to track how their confidential information gets disseminated throughout the supply chain and provides them with a comprehensive audit trail of who accessed the information and what operations were performed. The reports can be customized to be compatible with different databases or report generation applications

2.5 Access Rights Revocation

Bid-based procurement introduces another information security threat associated with sending RFP/RFQ to multiple suppliers. Even after the supplier is selected, all the other suppliers still have the confidential information in their possession. Probix Trustee rights revocation feature enables content owners to revoke access to the confidential information even after it was delivered to their suppliers.

2.6 Features and Benefits

- **Ease of use -** A most important design concept of Trustee is to preserve the business processes the content owner has in place. This concept led to a solution that is as transparent as possible to the content owner. It does not require the content owner to make any changes to the original content such as pre-convert it to a different format or move it to a different server. Probix Trustee is applied on-the-fly as the information is being delivered to the user.

- **Non-intrusive solution –**The solution is transparent to the end-user. It does not require pre-installation of any software on the user's workstation. The mobile code that is executed to enforce the content policies is delivered as part of the content.

- **Seamless integration** – Trustee can be seamlessly integrated into a corporation's existing environment and is interoperable with leading document management systems, access and authentication controls and corporate portals.

- **Support Static and Dynamic content** – Probix Trustee protects static, file-based content such as HTML, GIF, JPEG, PDF, Word documents, Excel spreadsheets, and PowerPoint presentations. It also protects dynamically created content such as HTML pages that contain information from databases through the use of Active Server Pages, Java Server Pages (JSP), CGI scripts etc.

- **Distributed and Scalable** - Probix Trustee network infrastructure is designed to scale to handle a high volume of transactions from geographically dispersed users. Content delivery is optimized by leveraging caching and Content Delivery Network (CDN) technologies.

- **Flexible Policies** – A wide range of user-based, action-based and time-based policies can be applied to a whole web site, specific directories, or individual pages. See section 3.2 for a complete list of optional policies.

- **Comprehensive Audit Trail** – Customized audit trail reports all accesses and operations performed on the protected information.

3. Technology and Architecture

3.1 How it Works

The following steps describe the process of content protection over the Probix Trustee network:

1. The content administrator assigns the content protection policies using a web-based tool provided by Probix. The tool provides a view of the web site content and the user database of individuals and user groups allowed to access that content. The administrator may also choose to create directories with pre-configured content policies into which publishers may publish the content directly.

2. When a user attempts to access the protected information, he/she is first authenticated by the customer's authentication system. The user's credentials are then examined by the customer's access control system and is either rejected or granted access to the information. Assuming the user has been given access permissions, the request is then re-directed to a Probix server. This re-direction is transparent to the user.

3. The Probix server examines the re-directed URL to check if that particular content already resides within its caching servers. The use of caching servers, which are designed to optimize performance over the Trustee network, is optional and can be configured by the customer.

4. If the content is not in the cache, the Probix server requests the content from the customer's web server. This is done over a secured link through either a VPN or an encrypted communication link provided by Probix. The content is then packaged in an 'ePouch', which contains the encrypted information, the policies and a mobile code.

5. The 'ePouch' is then delivered to the user. The mobile code is executed by the browser on the user's desktop, unwraps the content and displays it. The mobile code continues to run to enforce the content policies.

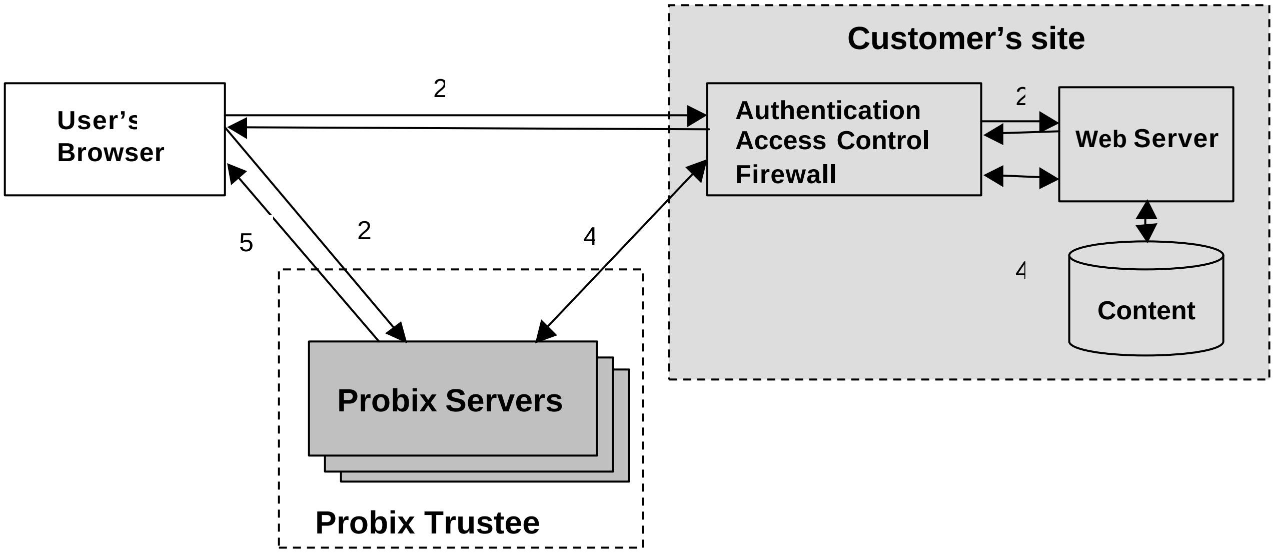


Figure 4. Theory of Operation

3.2 Probix Trustee Network Infrastructure

Probix Trustee infrastructure consists of a network of distributed server clusters deployed in co-location facilities around the globe. Each network node consists of clusters of servers and network devices dedicated to the following functions:

- Inter- and Intra-Node load balancing
- Content switching
- Dynamic URL processing
- Content retrieval & distribution
- Crypto engine
- Rendering engine
- Caching servers
- Policy management
- Key management
- Audit trail database

In addition to the load balancing within each node, Probix Trustee implements an inter-node load balancing to ensure a high availability, fault tolerant infrastructure. This robust, high performance, highly scalable architecture is designed to handle a large number of simultaneous transactions.

3.3 Authentication & Access Control

There are many different authentication mechanisms: user name and password, digital certificates, smart cards, secured tokens, etc. Probix Trustee interfaces with the customer's authentication system and retrieves the users credentials once they log in.

Similarly, there are different access control systems: domain level authentication, Access Control List (ACL), etc. Probix has partnered with numerous security providers to offer an integrated solution where web masters can centrally manage not only who can access the information, but also what they can do with it.

3.4 XrML

The Probix Trustee policy model is based on XrML, the evolving web standard for describing digital property rights. XrML provides a universal method for specifying rights and issuing conditions (licenses) associated with the use and protection of content. Probix-provided content-owners policy administration tools hide the XrML implementation from the administrator, while guaranteeing that the policy-management process fully benefits from the robustness, expressiveness and inter-operability provided by XrML.

3.5 Supported Content and Platforms

3.5.1 Server Platforms

Probix Trustee supports the following web server platforms:

- Microsoft IIS (NT 4.0, Win 2000)
- Apache (SUN Solaris, UNIX, Linux)

3.5.2 Client Platforms

Probix Trustee supports the following client platforms:

- Microsoft Internet Explorer and Netscape Navigator (Win 9x, NT4.0, Win 2000)
- Microsoft Explorer (MAC)
- Netscape Navigator (SUN Solaris)

3.5.3 Content Support

- Web Pages: HTML/XML
- Images: GIF, JPEG, TIF
- Dynamically Created HTML: ASP, CGI
- Documents: Word, Excel, PowerPoint, Adobe PDF