ThreatMetrix

WHITEPAPER

Trust Tags

Leveraging Shared Global Trust Intelligence to Enable Frictionless Authentication

All organizations with an on-line presence need to quickly and efficiently detect hackers and fraudsters. For e-commerce and online services, it's also essential to immediately recognize and establish trust with legitimate buyers and customers.

Advanced authentication procedures are necessary to reach both of these objectives. However, to avoid frustrating the very people you want to feel welcome, it's critical that the authentication process be as simple as possible.

Trust Tags are part of the next generation authentication technology from ThreatMetrix™. Without adding friction to the process of establishing trust, Trust Tags provide sophisticated and powerful intelligence to help organizations detect hackers and fraudsters, and speed up the process of trusting legitimate employees and customers .

Authentication for Fraud Prevention and Logon Protection

In the online world, there are two broadly related and often overlapping categories or uses that require advanced authentication – fraud prevention and logon protection. E-commerce sites detect and prevent fraud by using authentication procedures to authorize payments or other transactions. Online service entities need authentication to prevent the fraudulent use of stolen or fake identities during account creation, and to protect established logon accounts from being hacked and taken over. Additionally all enterprises with a remote workforce, regardless of size, need authentication to protect sensitive logon accounts from criminals and hackers.

Authentication is critical to establish the trust required to authorize transactions, and to protect logon accounts. But for businesses, the challenge is achieving the right balance of security and usability, at the right price (TCO).

Problem 1: Balancing Security and TCO

When implementing authentication for either fraud prevention or logon protection, organizations are faced with the challenge of balancing authentication strength with end-user convenience. Risk factors may necessitate secondary or out-of-band authentication at times, but these extra procedures can frustrate end users. So organizations need a sophisticated solution that challenges users with secondary authentication when necessary, but avoids doing so whenever possible.

However, creating a solution to accomplish this objective usually requires a custom database and other development, significantly increasing costs. This is due to secondary or out-of-band authentication systems not knowing when they need to be invoked—that depends on other risk factors. So organizations frequently need to develop something on their own to resolve that issue. Such a system requires a secure database to store user or customer authentication status, and ad-

vanced yet flexible rules and evaluation procedures to determine just when secondary authentication is necessary. But this can be a very complicated and expensive solution to create, particularly for organizations that don't specialize in authentication and fraud detection.

What many organizations need is a ready-to-go solution that works with their existing authentication systems and infrastructure, and adds the intelligence necessary to identify risky situations that require secondary authentication as well as detect trusted scenarios that don't. Furthermore, it would not require a custom database or extensive development to implement.

Problem 2: Maximizing Revenue While Minimizing Fraud

For organizations such as online services and e-commerce, the time it takes to trust a new buyer or customer is a critical factor. New customers may be accepting of extra authentication procedures or delays during their initial encounter, but the quicker they are recognized as a trusted consumer the happier they are, and the more likely they will return.

Unfortunately, establishing a high level of trust with new customers can take months. During that period, new consumers might be asked to repeat extra authentication steps, or even experience purchase restrictions. Either can be frustrating for new customers.

Furthermore, good customers frequently have their transactions denied because the merchant is unable to verify their trustworthiness. This results in frustrated consumers and lost business for the merchant.

If there is a way for merchants to know instantly that new customers can be trusted, and have the capability of maintaining that intelligence for future encounters, new consumers could make initial and subsequent purchases without friction. Customers and merchants would both benefit.

Trust Tags – Implementing Context-Based Authentication

In response to the challenges identified above, ThreatMetrix has added innovative technology and a corresponding set of features known as "Trust Tags." These new and advanced capabilities make it possible to instantly establish, preserve, and update granular levels of trust for each website or application visitor, whether that visitor is a remote employee accessing a sensitive application, a consumer at an e-commerce site, or a customer at an online services site.

Trust Tags serve as vital elements of intelligence that can be used to certify the level of trust, or non-trust, of individuals, devices, locations, user names, IDs, email and physical addresses, associated accounts, payment cards, and other authentication-related attributes. Trust Tags provide an important part of the central intelligence needed to mastermind and control the advanced authentication process, alleviating the need to craft custom solutions.

Trust Tags can easily equip web applications with powerful authentication capabilities for either fraud prevention or logon protection, challenging visitors or users with secondary authentication when needed yet providing smooth, frictionless authentication for trusted consumers, customers and application users. Trust Tags were specifically designed to help organizations achieve their security goals while reducing friction for their online customers and remote workforce.

Digital Labels Certifying Trust or Non-Trust

Every day ThreatMetrix profiles tens of millions of users and their devices, and regularly processes hundreds of millions of logins, payments, and other transactions. The ThreatMetrix Global Trust Intelligence Network is the secure repository for this wealth of real-time transactional data. This data includes information about users such as the set of email addresses they use, their various user IDs, ship to addresses, geolocation(s), their specific desktops, laptops, tablets, and smart phones, hashes of their payment cards and accounts, and other data that makes up their individual persona.

Trust Tags are digital labels that can be applied to the various user attributes or entities within the Global Trust Intelligence Network. Trust Tags certify the level of trust of these entities, providing advanced authentication capabilities for fraud prevention and logon protection.

For example, if an individual, say “Tom,” uses his laptop to access a ThreatMetrix-protected website (e-commerce site, online service, or enterprise application), and proves his identity during the session by passing a secondary authentication process, the site can apply a Trust Tag to Tom’s identity to indicate he is now trusted. The Trust Tag can specify details such as what sort of authentication Tom passed and when. During subsequent visits, the previously-applied Trust Tag certifies that Tom has already passed thorough authentication, therefore he can be trusted without subjecting him to another secondary authentication.

Trust Tags are not limited to individual elements. In our example, a Trust Tag could also be applied to Tom’s specific laptop, let’s say “Laptop X.” In fact, the real power of Trust Tags come from the ability to apply them to the combination of elements. In this case, Trust Tags would certify that “Laptop X” is a trusted device belonging to or used by Tom, a trusted user. Applying the Trust Tags instantly creates trust for the two entities when used together.

To expand our example, If Tom is accessing an e-commerce site and uses a specific payment card, if there is a high degree of confidence that it’s a valid card and Tom is the genuine owner, a Trust Tag could be applied to all three entities – Tom, his laptop, and a hash value uniquely identifying his payment card. During subsequent visits to the site, the Trust Tags would indicate that Tom, his laptop, and his payment card are all trusted when used together, and transactions could be instantly granted with a very high degree of confidence.

Trust Tags can be applied to any set or combination of entities. This provides very powerful and granular control, enabling organizations to approve or deny transactions or access to applications with an unprecedented level of control. For example, locations can be tagged as a trusted origin for specific user connections, or as trusted location(s) for shipments. IP addresses, URLs, email addresses, time frames, accounts, and essentially any entity that can be associated with one or more users can be tagged and used to direct and control the authentication process.

Our previous examples discussed positive trust. But Trust Tags can also indicate levels of un-trust. If Tom had failed secondary authentication, subsequent encounters with Tom would show the failure. If Tom's account were being attacked and had numerous authentication failures in a short period of time, Trust Tags would alert the protected application, revealing the number and time of the failures so the application can take appropriate measures. Another example of using Trust Tags to indicate negative trust would be tagging devices known to be infected with malware, or associated with botnets or fraudsters.

Trust Tags Can Be Private or Global

When ThreatMetrix applies Trust Tags, they are known as "Global Trust Tags", and are available to all organizations that use ThreatMetrix. All of the thousands of companies and enterprises that use the Global Trust Intelligence Network have full access to Global Trust Tags, and can use them in their authentication procedures to prevent fraud and protect logon accounts.

Trust Tags can also be applied by individual organizations. When this is done, they become "Private Trust Tags" and are only available to the company or organization that owns or applied the tags. No other company or organization can view or have direct access to the tags themselves.

Even though company A does not have direct access to Trust Tags owned by company B, company A can still benefit from Trust Tag intelligence provided by other ThreatMetrix customers. One example of this, is to have rules in place which evaluate how users and devices are being rejected or passed during login events globally in the network.

Trust Tag Applications and Uses

Trust Tags can be used in a many different ways, providing a multitude of fraud prevention and logon protection benefits for enterprises, e-commerce sites, and online service providers. The examples above focus on how Trust Tags can be applied to instantly establish user or customer trust so subsequent encounters don't require secondary authentication.

Here's a broader list of practical uses for Trust Tags. While a few of these examples pertain primarily to payment fraud, most apply to multiple applications, including remote workforce access, account takeover, and fraudulent account registration.

- **Establish immediate trust:** Trusted individuals can be instantly tagged, along with their devices, payment cards, and other attributes – significantly speeding up the process to establish a trusted reputation.
- **Identify loyal or VIP customers:** If a customer has a "loyalty card" or something equivalent, a Trust Tag can be set to immediately identify him as a trusted and welcome customer or user, thus avoiding secondary authentications.
- **Eliminate passwords:** For some lower-risk applications, a Trust Tag coupled with device identification might be all that's required, alleviating the need for a password.
- **Detect legitimate users in normally blacklisted regions:** Recognize when a legitimate individual is visiting a region that is normally blacklisted.
- **Track secondary authentications:** Tag user / devices combos that have passed or failed out of band authentication.
- **Track verified payments:** Answer questions like "Has this pair of payment account number + device ID had a verified payment in the last 90 days?"
- **Identify malware-infected devices:** ThreatMetrix identifies devices that have been infected with malware. Tagging such devices can help identify and prevent fraudulent usage.
- **Identify TOR network usage:** TOR networks are used to hide a user's location and other data. ThreatMetrix sets global Trust Tags when user IDs or devices are associated with TOR networks, helping to identify risk and reduce fraud.
- **Identify devices involved in attacks:** Tag devices when authentication fails. A large number of failures in a short period of time indicates the device may be owned or used by attackers.
- **Identify accounts under attack:** Authentication procedures can take appropriate action when accounts are tagged as repeatedly failing authentication within a short period of time.
- **Track groups of attackers:** Classify groups of attackers based on prior behavior and associations.
- **Track charge backs:** Tag users and or devices involved with charge backs to identify risks for future transactions.
- **Identify forgotten passwords:** Tag users who have failed authentication numerous times and have likely forgotten their password.
- **Detect devices associated with un-trusted geolocations:** Devices used in suspicious or un-trusted locations can be tagged as high risk.
- **Identify Valid Payment Cards:** Tag the combination of customers and their payment card identifiers when authenticated by services such as Verified by Visa or 2-D Secure.

The Bottom Line: Business Benefits of Trust Tags

Effective use of Trust Tags can result in many benefits, including:

- **Authentication system savings:** Minimal or no custom development and deployment
- **Better, stronger authentication solution:** Significant increase in security and flexibility improves fraud prevention, protection for IP, customer records, and brand reputation
- **Immediate establishment of trust:** No need to wait for days to months to build a reputation
- **Reduced user friction:** Simpler yet secure authentication results in happier workforce and customers
- **Increased revenue:** Legitimate buyers are recognized quicker, and not rejected
- **Increased productivity:** Remote workforce is granted easy but secure access
- **Reduced chargeback fees:** Improved fraud intelligence reduces bad transactions
- **Reduced internal costs:** Manual authentication reviews are reduced and simplified
- **Reduced external costs:** Need for out-of-band authentication is diminished
- **Reduced fraud costs:** Increased fraud and authentication intelligence minimize losses

Integration and Implementation

Trust Tags are set, checked, and updated through standard ThreatMetrix API calls. These APIs use the same syntax and methods ThreatMetrix customers are already using, so adding Trust Tags is straightforward.

Typical integration takes a couple of days, with API calls usually integrated within procedures that call secondary authentication systems such as challenge questions, Verified by Visa, one-time-password solutions, or other out-of-band authentication providers.

Since ThreatMetrix Trust Tags are part of the cloud-based TrustDefender™ Cybercrime Protection Platform, there is no other hardware or infrastructure required. Creating the calls to the ThreatMetrix APIs to set, check, update, or remove tags is all that is necessary to implement Trust Tags. This makes it extremely easy for organizations to achieve advanced, next-generation authentication capabilities, without having to develop sophisticated custom solutions.

ThreatMetrix™

Summary

The importance of trusting users and customers is often under appreciated, but it's vital if web site owners want to maximize their business opportunities. The quicker trust is established the better. Likewise, the more intelligence present about what creates that trust, the greater the opportunities and rewards.

Various technologies have evolved that help establish trust, from passwords to the addition of ThreatMetrix ExactID, SmartID, and advanced technologies like Persona ID. But even Persona ID requires time to establish the required level of trust, often a number of months.

Moreover, establishing trust frequently requires secondary authentication procedures, which can, if invoked frequently, be very annoying and frustrating. Regrettably, creating a solution that tracks secondary authentication to avoid its overuse typically requires web site owners to develop their own solutions – a time consuming and expensive process.

Trust Tags are an important component of ThreatMetrix next generation authentication capabilities and help solve these issues. They can manage secondary authentication data and calls and establish trust instantly, thus helping prevent fraud and protecting logon accounts. As an added benefit, Trust Tags make it possible to accomplish these objectives without web site owners having to create their own custom solutions.

Trust Tags are easy to implement, and offer many benefits, including:

- Lower costs to develop and deploy effective authentication
- Less friction for end users
- Reduced fraud and management costs
- Increased revenues for online services and merchants.

For more information, please visit us at:
www.threatmetrix.com

V3.13.2014