



Reputation is Everything

Device Reputation Authority™  
& iovation Reputation Services™

---

White Paper  
May 2007

## About This White Paper

iovation has pioneered a unique device reputation platform, called Device Reputation Authority (DRA), as a foundation for developing Internet based reputation systems. Today this platform is used by online businesses to successfully manage fraud, online abuse, and to control access to their networks and services using multi-factor authentication. The DRA maintains the reputation of millions of devices across the Internet. This white paper describes iovation's DRA platform and how it forms the foundation for developing reputation systems that help ensure the growth and integrity of the Internet as a trusted channel for businesses and consumers.

## Establishing Trust on the Internet— A Slippery Slope

The ability to associate an Internet user with a known identity, such as creating a set of attributes that uniquely identifies a user, is imperfect at best. As a result, there are several substantial hurdles facing online businesses today. For example, hijacked or forged identities allow fraudsters to pose as legitimate online users. Unfortunately, solving this challenge won't be sufficient to protect businesses and consumers who do business online without knowing the reputation associated with the users' identity.

Whether authorizing a purchase, granting access to personal financial information, enrolling a new partner or allowing someone the right to use a network, verifying user's identity and reputation are the two questions with which online businesses struggle. For the Internet to fulfill its potential as a trusted echo system, **reputation is the basis for that trust.**

## Building Device Reputation to Ensure Accountability & Trust

Trust is an expectation of future actions based on the reputation of some one or some thing. Trust is the foundation of commerce in the physical and online environments. In a paper published by Phillip Windley, Kevin Tew, and Devllin Daley of Brigham Young University, the authors propose that reputation is a currency or resource. Good reputation can translate into real economic value for an online business in the form of more customers while bad reputation could do the opposite. The same is true for consumers whose reputation could garnish trust and give them access to better service and discounts online while negative reputation could result in higher cost or even denial of access to services.

The iovation DRA platform helps aggregates feedback about a user's device to establish the reputation of Internet-enabled devices while protecting the identity of the users behind those devices. When a device is uniquely identified, it becomes possible to establish a reputation for it. A device's reputation is context sensitive and it conveys the types of behavior that has been associated with that device—good or bad. For example, devices that have been associated with confirmed fraud or predatory behavior in online communities carry a negative reputation in those specific contexts. An e-merchant site may only care about any reputation related to confirmed fraud while online communities would be more focused on keeping out predators.

Good reputation, explicit or inferred from known good transactions across one or multiple networks, indicates that the device and the identity behind it are more

*“A ‘trust ecosystem’ is an environment that engenders trust and accountability between people and businesses... trust must be extended to the Internet, and a key component, reputation, must cover not only individuals and organizations but also code and devices.”*

—Microsoft Press Release  
on Bill Gates Speech at RSA  
2006 February 14, 2006

trust worthy. A device's negative reputation is either built through direct evidence entered against it or inferred through its association(s) with other devices, accounts, and transaction where fraud has occurred. Therefore, it's vital to a reputation system to systematically uncover the web of associations (direct and hidden) among offending entities. Typically, associations among devices and accounts are formed when multiple devices access the same account or when multiple accounts are accessed using a single device.

With the ability to share information, even if a device accesses a Website for the first time, a reputation of negative behavior may be dynamically inferred and the device identified as suspicious. Both direct and association-based evidence against devices are maintained in the DRA, which is the underlying platform for iovation's Reputation Services.

## Device Reputation Sharing

Reputation sharing across subscribing online businesses means that good users can bring their good reputation along with them when visiting new sites so they are not strangers at first. For example, e-merchants can benefit by accepting more good orders while reducing the cost of manual reviews by knowing that a new user has a good reputation.

A device's negative reputation that is based on the experience(s) of one online business can help prevent the same device from causing problems over and over at the same site. However, if multiple online businesses participate in sharing the reputation and evidence they have collected on a particular device, then that shared reputation can help protect participating businesses against fraud from that device.

The DRA can dynamically identify any direct or indirect association(s) with past fraudulent activity, regardless of whether or not that past activity occurred on the network that is querying the system. It's this "reputation sharing" between networks that makes DRA-based solutions particularly effective in combating both existing and new account fraud, within or across industries, to proactively reduce fraud and abusive online behavior.

## Gaining Insights Through Decision Support

Decision support systems (DSS) have gained wide adoption over the last decade by giving businesses the ability to gain valuable insight to make decisions. The DRA repository, containing virtual identifiers for devices, accounts, transactions, along with other subscribers supplied identifiers (i.e. black lists), could help uncover hidden patterns and fraudulent associations embedded in the data to support business decisions and policies.

## A Solution Enabled by the DRA: Online Fraud & Abuse Management

Online fraudsters hide behind multiple virtual identities (hijacked or forged). As a result, iovation focuses on the online activities (good or bad) initiated from a device as opposed to focusing on the user behind the device(s).

Device Reputation Authority (DRA) enables online companies to combat fraud by focusing on the reputation of the user's device.

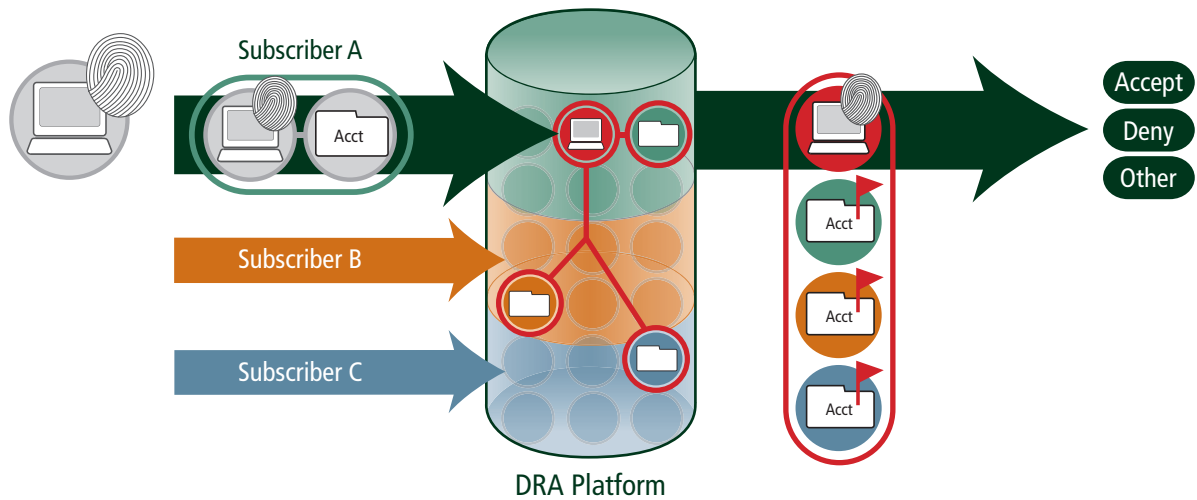
Using proprietary device identification technologies, iovation identifies the Internet-enabled device using a multitude of information supplied by the subscribing network without reliance on any Personally Identifiable Information (PII). Once uniquely identified, a reputation begins to be created for that device. Within the DRA, devices are associated with specific accounts or transactions using the information supplied by the subscribing network. The DRA maintains the relationships between devices, user accounts or transactions, along with fact-based confirmed fraud evidence entered against these entities by the subscribers.

When a device has been associated with confirmed fraud, such as chargebacks, or other negative behavior, such as chat abuse or online stalking, this evidence can be stored in the DRA repository to prevent further online transaction attempts on the subscriber's network from the offending device or its associated accounts and devices. In order to protect customer privacy, no personal identifiable information is maintained in the DRA.

As the foundation for the iovation Reputation Services, the DRA supports iovation Reputation Manager™ and iovation AccessManager™ online services:

- iovation ReputationManager is used to manage online fraud & abusive behavior
- iovation AccessManager provides strong multi-factor authentication and secure user access control

## How it Works



After a device has been associated with fraud or other bad/abusive behavior, evidence can be entered and stored in the DRA that contributes to the device's reputation to prevent further fraudulent online transaction attempts from the device.

## Solution Deployment and Interoperability

Solutions built on the DRA platform can be deployed stand-alone or can complement other fraud management and authentication approaches. Additionally, iovation's DRA can serve as a common repository and link evidence and identifiers from other fraud and authentication solutions to create a strong multi-contextual reputation management system. Conversely, the reputation of a device in the DRA can feed other fraud and authentication solutions that use a variety of factors to determine risk. The addition of device reputation provides physical, fact-based knowledge to approaches that otherwise rely on heuristics or behavior-modeling techniques.

## DRA and Personal Privacy

A common approach to online user authentication and combating fraud is to make the user go through more intrusive procedures when transacting online. Consumer reactions to the use of sensitive personal information range from justifiably concerned to truly activist. One advantage to DRA is that it does not require the retention or use of any personal information.

DRA does not rely on personally identifiable information (PII) because it enables the unique identification of an online user's device as it accesses and transacts within and across networks as opposed to focusing on identifying the user as a person. DRA's focus on the device and its reputation rather than the person behind the device protects the user's privacy.

For more information on iovation's DRA-based solutions for fraud management and authentication, visit [iovation.com/products](http://iovation.com/products).