bioChec ™

Keystroke Biometric Solutions

Physical Biometrics

- Defined as the statistical analysis of biological observations and phenomena

- Characteristics:
  - Measurement of biological aspects of a person that determine identity
  - Static measurement
  - Absolute match

- Examples:
  - DNA, Retina, Fingerprint, Vein structure

Behavioral Biometrics

- Defined as the collection and classification of a series of intrinsic patterns displayed

- Characteristics:
  - Measurement of characteristic traits exhibited by a person that can determine identity
  - Dynamic measurement
  - Confidence match

- Examples:
  - Speech Recognition, Handwriting Analysis, Keystroke Biometrics, Facial Recognition

Software-Only Biometrics

bioChec

"Keystroke Biometrics" is a behavioral biometric which creates a statistically unique signature from the typing patterns of an individual without the use of specialized hardware.

Keystroke Biometrics is a proven technology:

- **1979**: Technology originally developed by SRI International.
- **1980**: National Bureau of Standards (NBS) study concluded that computer keystroke authentication of 98% accuracy.

...

- **2009**: bioChec granted U.S. Patent 7,509,686

Statistical Confidence Levels

bioChec

Fingerprint

- Physical biometric
  - FAR= ~0%
  - FRR= ~1%
- Uniqueness= 1 : 298023223876953125 0x1024

Keystroke Biometrics

- Behavioral biometric
  - FAR = ~ 0.01%*
  - FRR = ~3.0%*
  - Crossover Rate = ~1.6%*
- *Tweakable, Application-Defined

Facial Recognition

- Physical biometric
  - FAR / FRR vary significantly according to compression, distance, illumination, media, pose, resolution, and other temporal factors.

Voice Recognition

- Behavioral biometric
  - FAR = ~1.6%
  - FRR = ~8.1%

Software-Only Biometrics

bioChec

Deploying software-only keystroke biometric solutions into an existing network infrastructure is a seamless and cost-effective way to augment corporate security.

- No physical client-side deployment for installations or upgrades.
- Users are not limited to individual or specific workstations.
- Server and/or workstation managed levels of security.
- Software components allow integration into multiple projects.

bioChec ™ as a Solution Provider

bioChec™ addresses both product and service areas of biometric solutions

bioChec™ provides a patented software-only biometric technology that is minimally invasive and easily deployable to a large community of users.

bioChec™ provides SaaS fulfillment service for enhanced security solution provider implementations.

Product Offerings

bioChec

Custom Application Development

- **bioChec**Key™ Keystroke Biometrics SDK

Web-Based Intranets and Extranets

- **bioChec *Online!*** ™

Legacy Applications:

- **bioChec *GINA!*** ™

bioChecKey ™ Biometrics Engine

bioChec

Software-Only SDK

- Win32, Linux or Unix, Java (via JNI)

Dialog Input Field Hooks (Win32, QT3, QT4, X11)

- Allows Rapid Application Development

Adjustable Verification/Enrollment Parameters

- Tweak Implementations to your needs

Expirational Encryption™ Technology

- Limits data decryption to N seconds to prevent stream hijacks

Adaptive Template™ Technology

- Increases Template Strength with every successful login

Dynamic Enrollment™

- For Initial Deployments, negates need for explicit enrollment

Password Hardening (bioChec GINA! only)

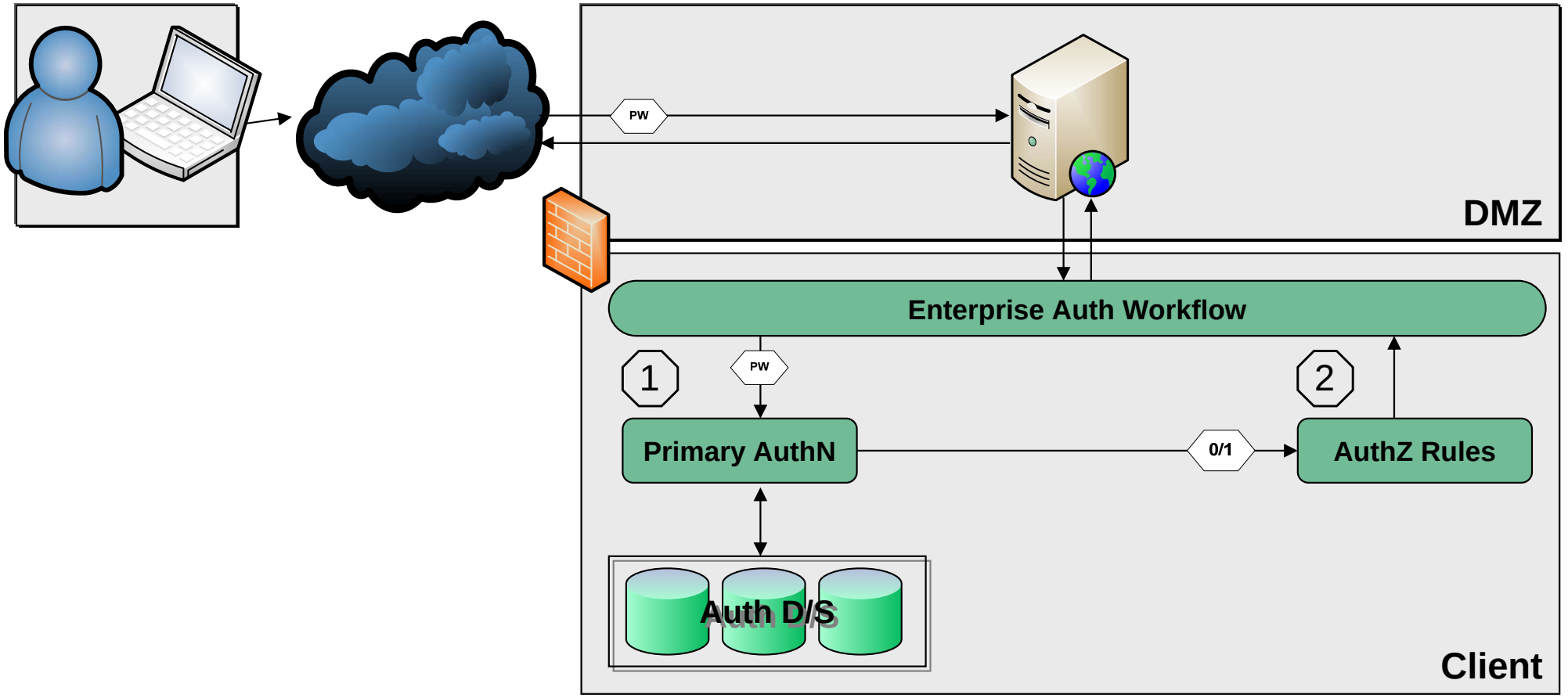
- Replaces normal password with a bioChec-only password.
- Prevents all non-bioChec authentication (even Windows® Repair Console).
- Can recreates a new random password on every template update.
- Effectively isolates Windows® workstation from incoming access.

Online Authorization

- Non-Invasive Client-Side deployment
  - Flash
  - Java Applet
- Simple integration into existing infrastructures
  - WS-*
  - SaaS
  - Custom
- Administrative Features
  - Adjustable Verification / Enrollment Parameters
  - *Adaptive Template*™ Technology
  - *Dynamic Enrollment*™ option
- Security Features
  - *Expirational Encryption*™ Technology
  - Playback Resistance
  - PKI (RSA or Diffie-Helmann) encryption

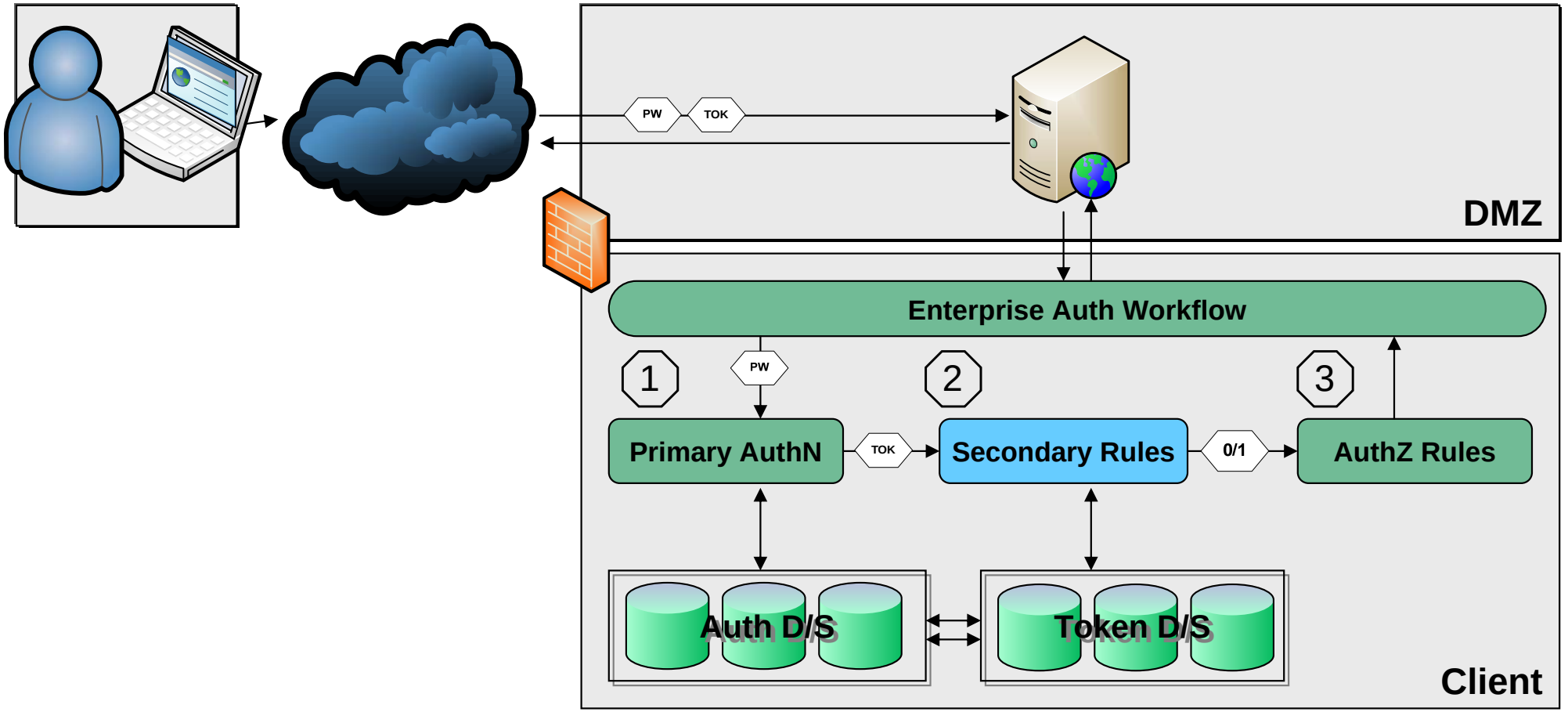
Basic Authentication Model

bioChec



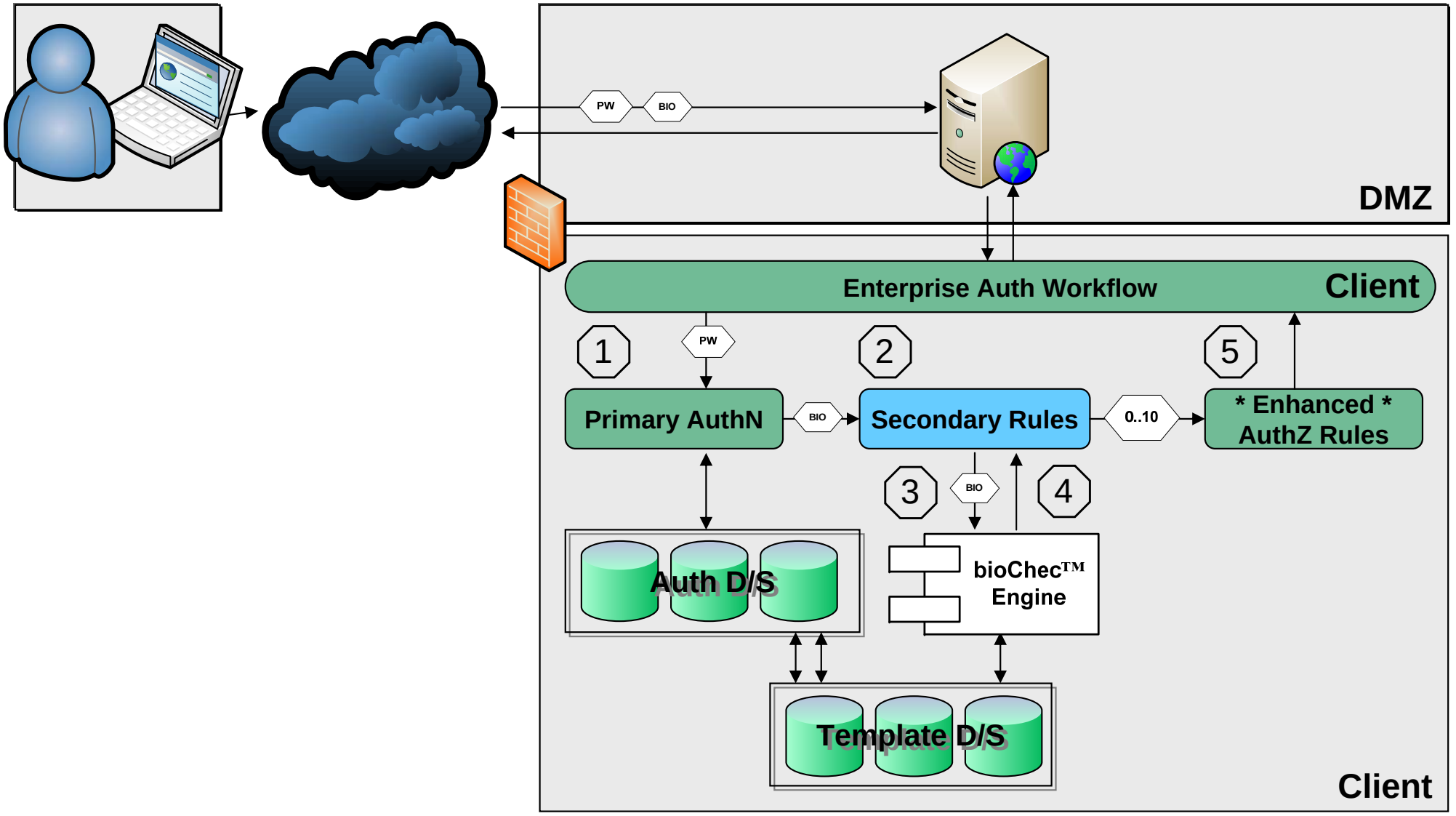
Token Authentication Model

bioChec



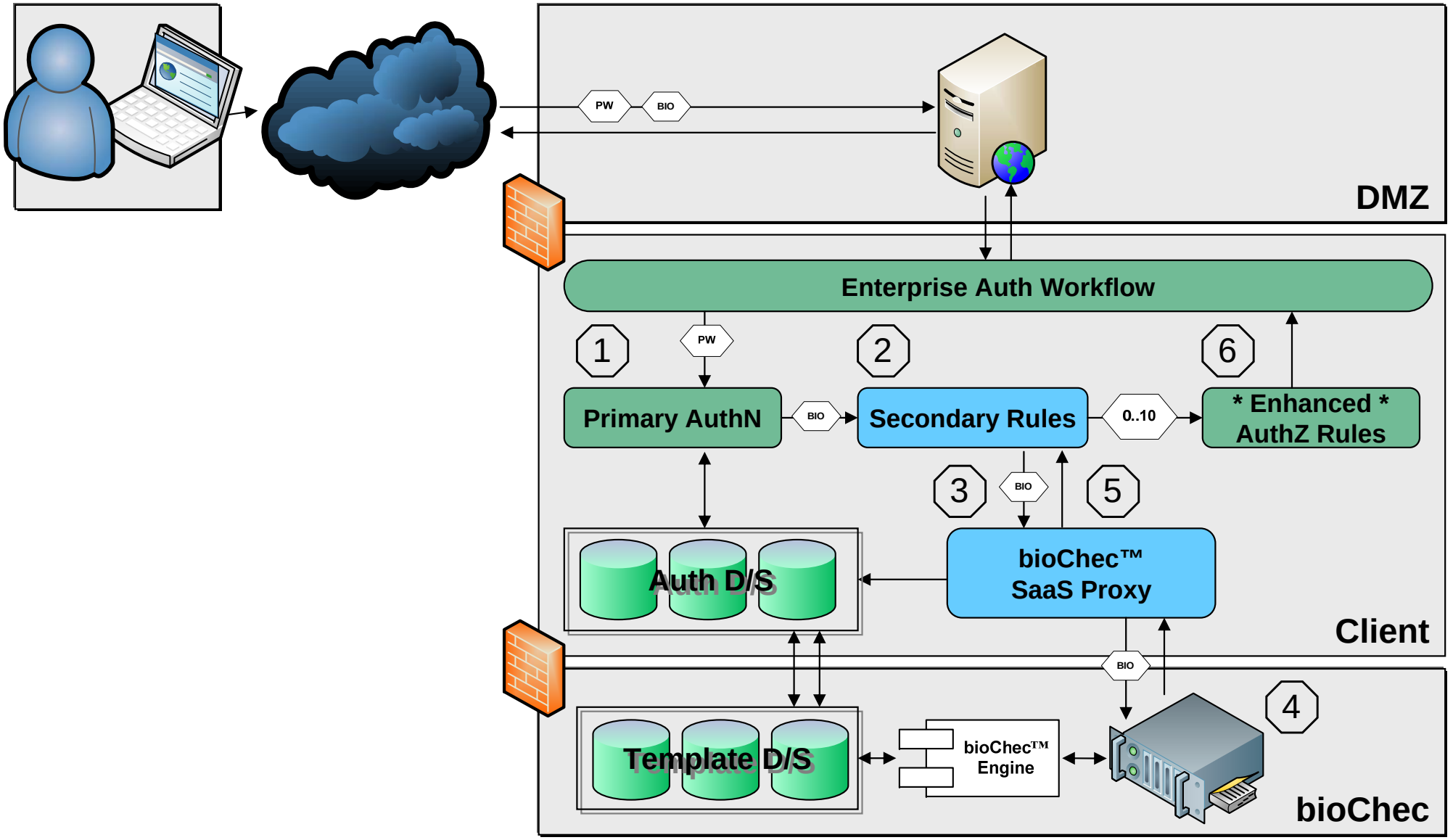
bioChec Integration Model

bioChec



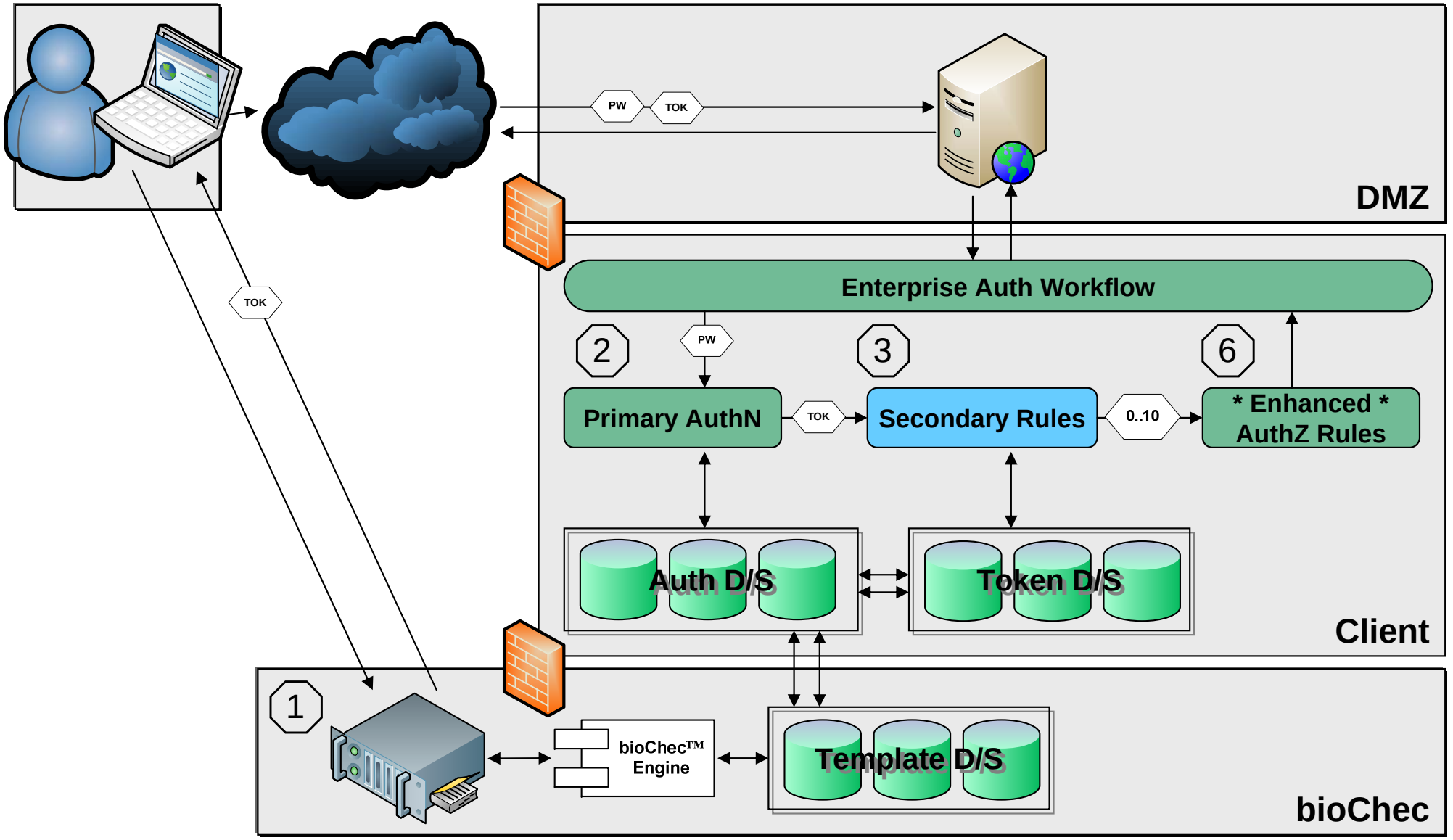
bioChec SaaS Model

bioChec



bioChec Broker Model

bioChec



Ad-Hoc auditing for rogue workstation access

bioChec's profile algorithm allows ad-hoc auditing of typing snippets.

Profiling, although not as accurate as templates, may be used to determine sudden changes in typing behavior.

These sudden changes may be attributed to a disparate user executing commands on another person's workstation.

Extensions to the profiling algorithm will, in the future, be able to aggregate these disparities across an enterprise and possibly identify individuals consistent with the rogue access attempts in question.

Secure Software Licensing and Registration.

The future of this technology can be seen in secure product registration. The idea behind this will help prevent piracy, and create an audit trail for any piracy breaches.

As a simple scenario, a user purchases a software package online.

- *Within the purchase process, the user is asked to enroll [online] a biometric (keystroke-dynamics-based) signature and is returned a single-use installation key.*
- *Upon installing the actual software, the user is asked to verify their signature against this key.*
- *This verification process destroys the original template and produces a runnable license tied to a combination of the specific installation (hard disk serial, CPU serial, NIC, MAC, et al) and user (signature Hash).*