



CYBER SAFETY HARBOR

SECURING CIVILIAN CYBERSPACE BEYOND DOD SPECIFICATIONS

Cyber Safety Harbor (CSH)'s products are a quantum leap in securing sensitive transactions on the Internet. Our patented system engages a new mindset in security; instead of reactive "patch-and-repair," CSH takes a new approach of reducing the universe of users, then engaging security **before the portal is created**, not after as is current methodology. This "disruptive technology" with incredible market potential.

The primary product hardware, IsoNuclei, currently in USB formfactor, contains both a Hardware Unique Factor (HUF) and a Secure Execution Environment (SEE) used to establish PRESENCE over cyber. Originally designed for US Military Command and Control, CSH holds the patent on SimulNuclei which defines a set of IsoNucleis with authorization to perform a set of actions and then a subset of those whose presence must be established in order to perform one of those actions.

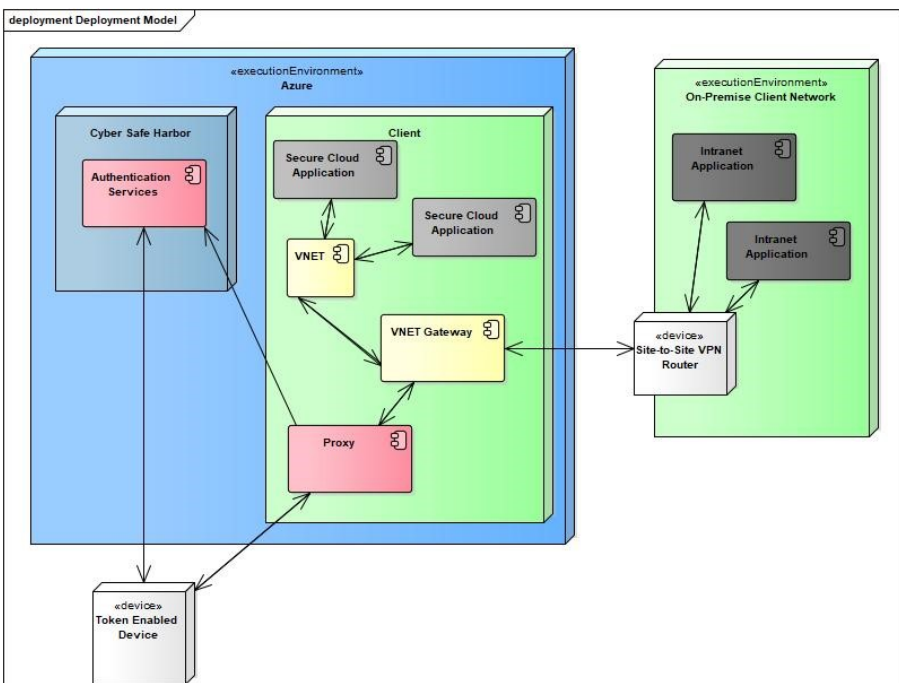
A HUF is crypto-etched silicon that is theoretically physically impossible to duplicate once etched meaning, once registered with CSH's authentication services, only that specific IsoNuclei has the ability to authenticate. SEE's enable software to run in the memory space on the IsoNuclei itself, not on the Host OS, and therefore, since nothing is in RAM on the underlying computer, once the IsoNuclei is removed the session implodes and not only does the user lose access to the application but also there is no evidence of their session on the host computer, since there was none to begin with.

APPLICATIONS IN THE LEGAL FIELD

The initial market for IsoNuclei is projected to be Law Firms, particularly those in Mergers & Acquisitions. M&A Firms have increasingly been targeted for their documents, which are regularly accessible through "secure" web portals that this technology would eliminate. The cost-benefit ratio is high here as a single leak could cost billions and implementing this solution on top of something like SharePoint is trivial from both a technical and logistics standpoint.

APPLICATIONS IN PRIVATE BANKING

In private banking SimulNuclei could be applied to account actions like wire transfers where both the account holder and a banker both need to establish presence, perhaps the banker even at a physical location. This maintains the human authentication element many banks now require for some transactions while the transactions remain available in cyberspace.



The solution on the left is a next-generation implementation of CSH's original co-located plan. In this CSH's Authentication Services are deployed on Azure, first in a Virtual Machine and later as true PaaS solution where private authentication providers can be deployed.

The client then has deployment in Azure including a Proxy specifically designed to talk to the authentication services and relay web application back to the 'Token'. Behind the proxy will sit a VNET that connects Site-to-Site with the client's physical infrastructure for the proxy to access. The Proxy will be a packaged network component so that the client can be deployed, and marketed, under a true IaaS model.