SAY**FUSE** Infrastructure Appliance

Die All-In-One IT-Sicherheitsinfrastruktur für Ihr Unternehmen

SAYTEC

Inhaltsverzeichnis

1. Vorwort

Die zunehmende Digitalisierung durchzieht unseren Alltag. Sie bietet neue Möglichkeiten für die Gesellschaft, weist aber auch Risiken auf. Durch die Vernetzung nahezu aller Lebensbereiche erhalten wir stetig mehr Zugang zu digitalen Infrastrukturen, Dienstleistungen und Datenquellen, mit denen wir ständig interagieren. Sie erleichtern in vielen Bereichen unser Leben, z.B. bei der medizinischen Versorgung und verbessern die Nutzung erneuerbarer Energien – dadurch steigen jedoch der Datenbe^darf und der Datentransfer rasant.

Für viele Firmen sind Daten der wesentliche Teil ihres Unternehmenswertes. Jederzeit können durch technisches Versagen, Anwenderfehler, Angriffe oder Manipulationen gespeicherte Daten verloren gehen, IT-Systeme zusammenbrechen oder unbrauchbar gemacht werden. Die Betriebsfähigkeit und die Markpräsenz eines Unternehmens sind heute in hohem Maße von IT-Systemen abhängig. Deshalb müssen Netzwerke, Daten und Anwendungen gegen mögliche Gefahren geschützt werden. Viele Betriebe begegnen der drohenden Gefahr leider nicht mit der notwendigen Ernsthaftigkeit, obwohl in Deutschland die Absicherung von Daten auch gesetzlich vorgeschrieben ist.

Schlagzeilen über verheerende Cyberangriffe nehmen zu. Eine Betriebsunterbrechung kann ein mittelständisches Unternehmen mehrere hunderttausend Euro am Tag kosten. Untersuchungen zeigen, dass bis zu 70 % der Unternehmen nach einem Störfall oder Angriff ihre Daten nicht wiederherstellen konnten. Dabei zeigt sich, dass viele Angriffe oder Betriebsunterbrechungen durch eine konsequente Datenschutz- und -erhaltungsstrategie und eine angesicherte IT-Infrastruktur vermeidbar wären.

In einigen Branchen bildet die Speicherung sehr großer Datenmengen und die aktive Nutzung dieser Daten den Kern ihrer Dienstleistung. Bei der medizinischen Versorgung oder Pilotenausbildung bspw. werden riesige Datenvolumen während Computer- und Magnetresonanztomographien oder Flugsimulationen generiert und laufend auf- und abgerufen.

Herkömmliche Storagelösungen oder Bandsystem Technologien können die notwendigen Anforderungen bei der Datensicherung nicht mehr umfänglich erfüllen. Sowohl die Technologie der Storage- als auch der Bandsysteme weisen Vor- und Nachteile in Bezug auf Back-up und Restore auf. Beispielsweise können bei Storage basierten Technologien Hardwaredefekte oder auch Schadanwendungen und bei Band basierten Systemen die Umgebungseffekte wie Temperaturunterschied Datenverluste zur Folge haben.

Die ideale Lösung muss daher die vorteilhaften Eigenschaften beider Technologien vereinen und die Nachteile innerhalb der gesamten Infrastruktur ausschließen. Genau das erreicht die SAY**FUSE** Backup- und Restore Plattform mit ihrer patentierten Technologie.

2. SAYFUSE Infrastructure Appliance Ihre neue IT-Sicherheitsinfrastruktur

Unternehmen sind heutzutage mit weitreichenden Anforderungen konfrontiert. Sie müssen eine Vielzahl von Diensten und Systemen für ihre Mitarbeiter und Kunden in ihren Netzwerken zur Verfügung stellen. Gleichzeitig müssen sie sich vor externen Angriffen schützen und ihre IT-Infrastruktur und Anwendungen laufend pflegen.

Sie tragen die volle rechtliche Verantwortung und können diese nicht an Dritte übertragen. Das Sicherheitskonzept umfasst den Zugriff auf Firmennetzwerke, die Datensicherung, die Zugangssicherung, die Ausfallsicherheit und die Datenverfügbarkeit.

Im Fokus steht dabei immer eine funktionierende IT-Infrastruktur, in Verbindung mit einer verlässlichen und leistungsfähigen Sicherheitsarchitektur unter Berücksichtigung der branchenspezifischen Bedürfnisse.

Mit der SAY**TRUST** Infrastructure Appliance bieten wir Ihnen einen sicheren Zugang zu Ihren Unternehmensdaten und eine hochsichere Arbeitsumgebung. Zudem bietet die Appliance eine einfache und verlässliche Backup Lösung, die eine reibungslose Wiederherstellung im Bedarfsfall sicherstellt. Dabei werden sensible Daten und die Vernetzung hochkritischer Infrastrukturen abgesichert.

- Backup und Restore für Primär- und Sekundärsicherungsvorgänge
- Serverplattform für primäre und sekundäre Anwendungsfälle
- Hoch performante Server- und Daten-Storage-Systeme
- Internen Nerzwerkschutz des Netzwerkes gegen Missbrauch
- Hochsichere Remote-Access-Zugänge für Heim- und mobile Arbeitsplätze
- Hochsichere Kommunikationsplattform für Mitarbeiter und Unternehmen
- Virtuelle Client-Rechner für die allergen- und geräuschfreie, hardwareunabhängige Arbeitsumgebung

2.1 Das SAYTEC Sicherheitskonzept

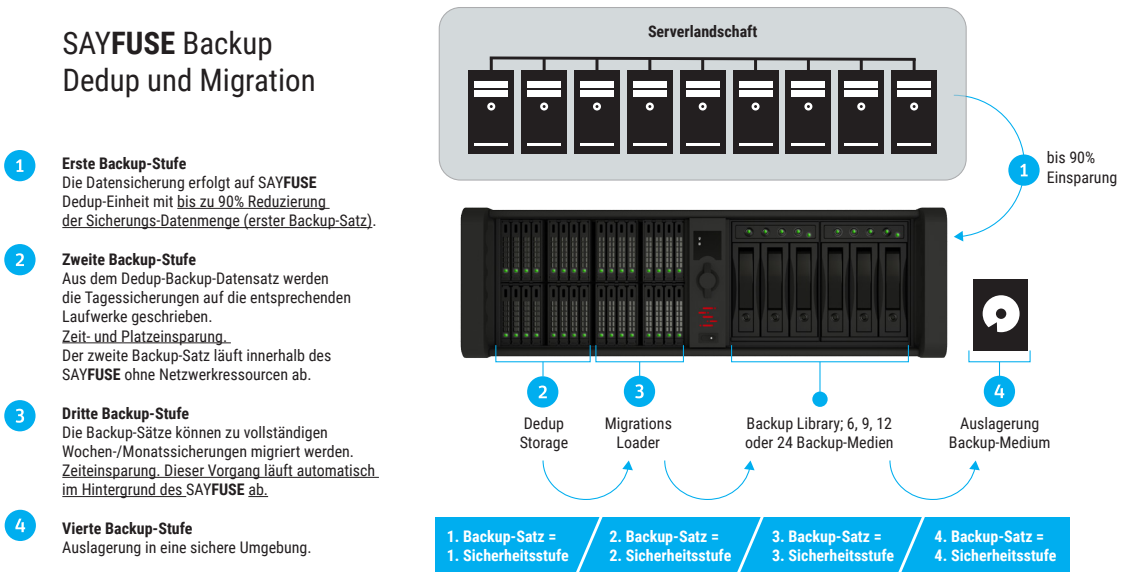
Die SAY**FUSE** Appliance ist so konzipiert, dass alle Compliance-Richtlinien innerhalb des Systems erfüllt werden. Mit seinem Vier-Stufen-Generations-Sicherungssystem vereint SAY**FUSE** alle vier grundlegenden Stufen einer zuverlässigen Sicherungsstrategie innerhalb eines Systems. Durch die Sicherung und Wiederherstellung von Multi-Backup-Laufwerke, Multi-Stream und Migration wird die Geschwindigkeit überdurchschnittlich erhöht. Viele Terabytes an Daten können innerhalb weniger Stunden gesichert und in eine geschützte Umgebung auslagert werden.

Stufe 1

In der ersten Stufe beginnt die Datensicherung mit einer echten vollständigen Sicherung in den Backup-Dedup-Storage innerhalb des SAY**FUSE**. Das spart Zeit, reduziert die Netzwerkbelastung bis zu 90% und bildet den ersten Sicherungsdatensatz.

Stufe 2

In der zweiten Stufe wird jobgesteuert das dafür konfigurierte Backup-Laufwerk eingeschaltet und die Tagessicherungen werden innerhalb der SAY**FUSE** Appliance aus dem Backup-/Dedup-Pool auf die entsprechenden Medien migriert. Nach Abschluss der Sicherung wird das Sicherungslaufwerk abgeschaltet. Dieser Vorgang findet ohne externen Zugriff statt, spart Zeit und schont die Netzwerkressourcen.



Stufe 3

In der dritten Stufe migrieren die Backup-Sätze automatisch im Hintergrund (innerhalb der Appliance) mit den täglichen Änderungen in die wöchentlichen bzw. monatlichen Vollsicherungen. Dabei werden die jeweils dafür konfigurierten Backup-Laufwerke mit dem Backup-Job eingeschaltet und die Backup-Medien auf Konsistenz geprüft. Nach Abschluss der Sicherung wird das jeweilige Backup-Laufwerk abgeschaltet und die

Sicherung für die Auslagerung bereitgestellt. Das schützt die Sicherung vor Angriffen, spart Energie und erhöht die Lebensdauer der gesicherten Daten.

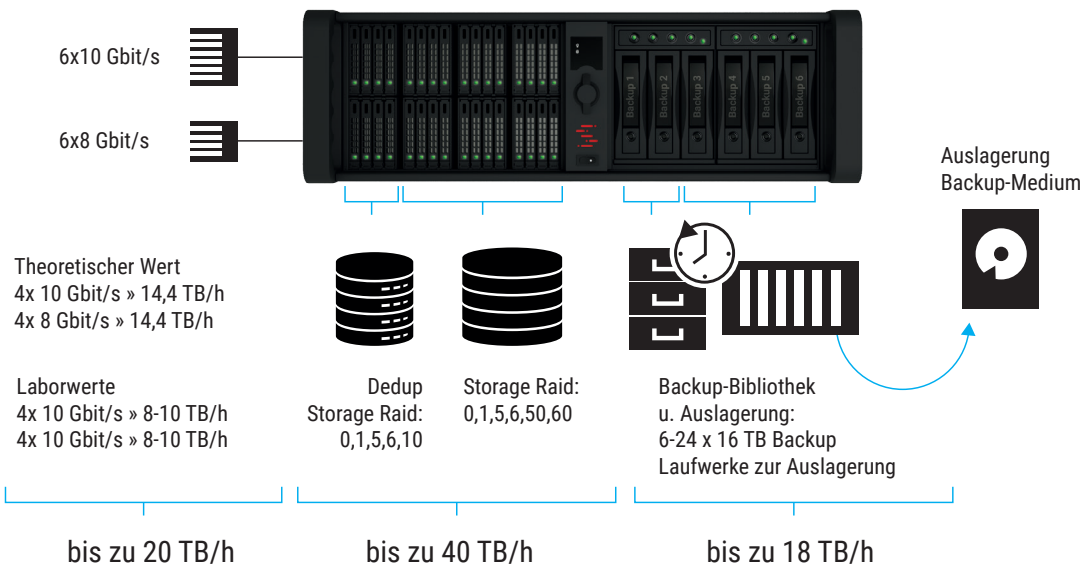
Stufe 4

Die Auslagerung ist die vierte Stufe. Auf Knopfdruck können Sicherungsmedien als Voll-Sicherungssätze aus den Sicherungslaufwerken entfernt und in eine geschützte Umgebung ausgelagert werden. Unternehmenssicherungen beinhalten Geschäftsgeheimnisse und personenbezogene Informationen. Sie müssen verschlüsselt, vor unbefugtem Zugriff geschützt an einen sicheren Ort oder weiteren Brandabschnitt ausgelagert werden.

2.2 Daten-Transfer-Kapazität

Die Datenübertragungskapazität, d.h. die Menge der digitalen Daten, die über einen bestimmten Zeitraum in einem Übertragungskanal transportiert werden, hängt von vielen Faktoren ab. Für ein durchgängiges Backupkonzept müssen sämtliche Faktoren berücksichtigt werden. Für die Sicherung großer Datenmengen, deren Replikation und Auslagerung müssen alle Schnittstellen, die Topologie sowie Storage- und Sicherungslaufwerke für die Auslagerung berücksichtigt werden. Im Zeitalter großer Datenmengen ermöglicht der SAY**FUSE**, 100 TB Daten oder mehr an einem Tag oder Wochenende auszulagern und für die Rücksicherung verfügbar zu machen.

SAY**FUSE** Backup
Datenübertragungskapazität



3. Sicherer und einfacher Zugriff

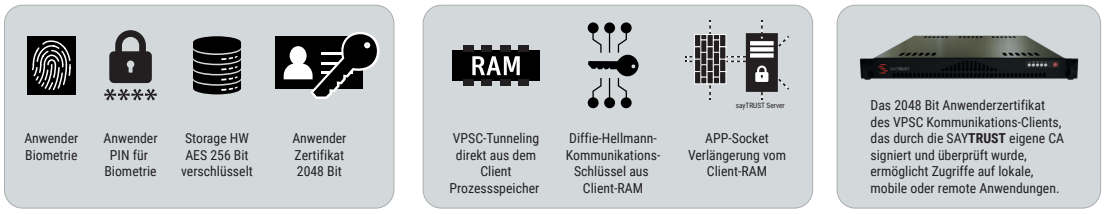
Im Gegensatz zu VPN Technologien setzen die Sicherheitsmechanismen bereits vor dem Kommunikationstunnel ein. Dies geschieht durch den koordinierten Einsatz mehrerer ineinandergreifender Sicherheitsstufen (Defense in Depth). So werden Daten und Netzwerk in höchstem Grad geschützt. Das vielschichtige Abwehrsystem minimiert die Risiken und die Möglichkeiten eines Ein-dringens exponentiell im Vergleich zu VPN-Lösungen. Sollte es einem Hacker dennoch gelingen, eine der Sicherheitsbarrieren zu überwinden, so wird der Zugriff durch die weiteren Sicherheitsstufen unterbunden. Nur wenn sämtliche ineinandergreifende und voneinander abhängige Sicherheitsstufen durchlaufen werden, wird die sichere Kommunikation aufgebaut.

Hierbei sind die Sicherheitsstufen in drei Sicherheitsblöcke unterteilt:

- Sicherheitsblock 1: Sicherheit durch eindeutige persönliche Identifizierung
- Sicherheitsblock 2: Verbindungssicherheit durch Defense in Depth
- Sicherheitsblock 3: Sicherheit durch Netzwerk-Zugangs-Kontrolle

3.1 Sicherheit durch eindeutige Identifizierung:

SAY**TRUST** VPSC Kommunikationssicherheit



Sicherheitsblock 1
PKI mehrstufige Persönliche Identifizierung.
Sicherheit vor Aktivierung des Clients

Sicherheitsblock 2
Verbindungssicherheit Defense in Depth.
Sicherheit vor der Kommunikation

Sicherheitsblock 3
Überwachung durch SAY**TRUST** Server
vor dem Netzwerk

Bevor der SAY**TRUST** Access Client auf einem PC oder einem Notebook in Einsatz kommen kann, wird die Identität des Benutzers mehrstufig überprüft:

1. Die Anwender-Biometrie dient zur eindeutigen Identifizierung des Anwenders und zur Aktivierung des SAY**TRUST** Access USB-Clients (ausschließlich bei biometrischen Clients). Erst nach der eindeutigen Identifikation des Anwenders wird der SAY**TRUST** Access USB-Client von dem jeweiligen Arbeitsrechner erkannt (bei Mikrochip basierenden Clients) und startet automatisch den zweiten Identifikationsschritt, den

2. AES verschlüsselter Anwender-Storage. Der 256 Bit AES verschlüsselte Bereich dient dem Schutz der mobilen Anwendungen und Dokumente. Aus diesem Bereich heraus wird auch das SAY**TRUST** Anwender-Menü gestartet. Es stellt entsprechend

den Berechtigungen des Nutzers die lokalen, mobilen und remote Anwendungen, sowie Netzwerk-Ressourcen bereit und leitet den dritten Identifikationsschritt über das 2048 Bit Anwenderzertifikat ein.

3. Das Anwender-Zertifikat überprüft, ob das Ursprungs-Zertifikat verändert wurde und ob der Anwender von seinem aktuellen Standort aus einer Kommunikation aufbauen darf. Zusätzlich gleicht es die Berechtigungen des Benutzers für sei-ne Unternehmens-zugriffe mit dem SAY**TRUST** Server ab. Danach überwacht der SAY**TRUST** Kommuni-kations-Client aus dem Prozessspeicher (RAM) die Nutzung, indem er die jeweiligen Anwendungen gezielt tunnelt, blockiert oder abkapselt. Eine ungewollte Schad- oder Spionagesoftware gelangt so nicht in den Tunnel.

4. Der Anwender-PIN. Das Zertifikat wird durch den Anwender-PIN zusätzlich ge-schützt. Diese transparent ablaufende mehrschichtige Prüfung der Identität verhindert den Zugriff eines Angreifers weit vor dem Kommunikationsbeginn. Nach erfolgreichem Abschluss des ersten Sicherheitsblocks setzt sich der SAY**TRUST** VPSC-Kommunikati-ons-Client in den Prozessspeicher. Damit startet der zweite Sicherheitsblock.

3.2 Verbindungssicherheit mit VPSC

1. Der VPSC-Kommunikations-Client überprüft im Prozessspeicher anhand des 2048 Bit Anwenderzertifikats, das durch die Certificate Authority (CA) des SAY**TRUST** Access Servers erstellt wurde, die Zugriffe auf lokale, mobile oder remote Anwendungen und Ressourcen. Nur erlaubte Anwendungen werden getunnelt. Nicht erlaubte Anwendun-gen werden blockiert. Bevor jedoch eine Kommunikation mit den zu schützenden Res-sourcen (Anwendungen, Server, Netzwerk, …) zustande kommen kann, wird in Abhängig-keit des Anwenderzertifikats ein

2. personifizierter, client- und serverseitiger Perfect Forward Secrecy Schlüssel (PPFS) für die Kommunikation zwischen dem SAY**TRUST** Client und SAY**TRUST** Access Server ausgehandelt. Der in Abhängigkeit des Anwenderzertifikats neu generierte - bis zu diesem Zeitpunkt weder dem Client noch dem Server bekannte Schlüssel - wird für die zukünftige Kommunikation verwendet. Dabei wird der

3. Socket der Anwendung direkt vom Arbeitsspeicher des Clientrechners zu dem/der zu schützenden Netzwerk/Ressource getunnelt. Der Client-PC kann sich in einer un-sicheren Umgebung befinden und stellt das schwächste Glied in der Kommunikations-kette dar. Im Gegensatz zu herkömmlichen VPN-Technologien wird bei der SAY**TRUST** Lösung der Client-PC kein Mitglied des geschützten Netzwerks. Die durch SAY**TRUST** Access aufgebaute VPSC-Verbindung erfolgt aus dem Arbeitsspeicher in der Anwen-dungsschicht. Informationen des geschützten Netzwerkes werden nicht auf dem Client-Rechner vorgehalten und sind weder auf dem Client-Rechner noch auf der Verbindungs-strecke sichtbar. Wird die Verbindung beendet, verbleiben auf dem Client-PC und auch auf der Kommunikationsstrecke keinerlei Informationen zurück.

3.3 SAYTRUST Server

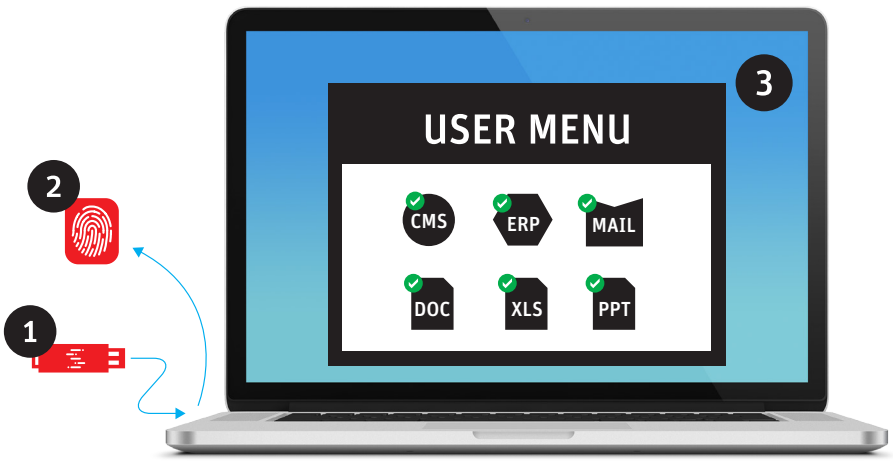
Der SAY**TRUST** Access VPSC Server enthält den Certificate Authority (CA) Server. Er wird bei der Installation des SAY**TRUST** Servers für das Netzwerk eingerichtet. Der CA-Server ist für jedes Netzwerk, das durch die VPSC-Technologie geschützt wird eindeutig und akzeptiert ausschließlich eigene Zertifikate. Alle Zugriffsversuche werden durch den überwacht, nach Prüfung des Anwenderzertifikats wird der Zugang entsprechend der Berechtigungen des Anwenders gewährt. Alle anderen Versuche werden verworfen.

3.4 SAYTRUST Access - einfache Bedienung für den Anwender

Für Anwender ist die Bedienung der SAY**TRUST**-Zugangslösung sehr einfach und flexibel in der Nutzung (siehe Abbildung).

Direkt nach dem Einstecken des SAY**TRUST**-USB-Access-Clients in den PC (1) erfolgt die persönliche Identifikation (2).

Nach erfolgreicher Identifikation startet das SAY**TRUST**-Menü des Anwenders (3). Benutzer- und Remotenetzwerkspezifische Informationen werden im Arbeitsspeicher erstellt und verwaltet. Nach Beendigung der Kommunikation werden diese gelöscht, es verbleiben keine Spuren auf dem PC.



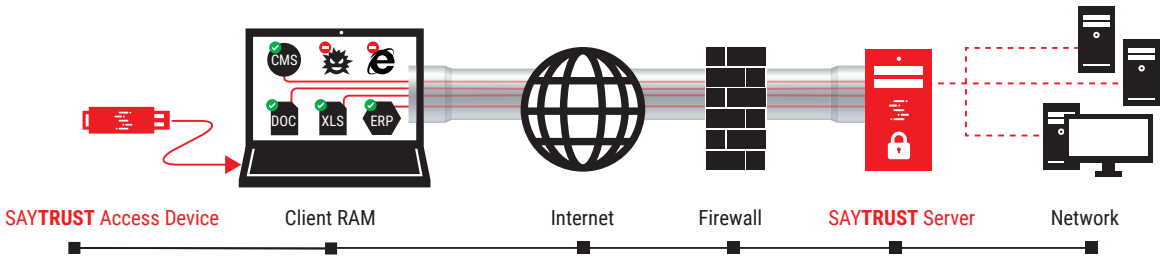
3.5 Zugriffssicherheit für Kunden

Der Kunde loggt sich mit SAY**TRUST** Client von einem beliebigen Rechner aus ein. Die Anfrage wird zum SAY**TRUST**-Zugriffsserver weitergeleitet und mit den Registrierungsdaten abgeglichen. Der SAY**TRUST**-Kunden-Client baut dann nach erfolgreicher Authentifizierung den SAY**TRUST** Tunnel auf.

SAYTEC bietet umfassende Schulungsprogramme für Anwender, Administratoren, technisches Supportpersonal und Mitarbeiter von Systemintegratoren.
Schulungen, Workshops und Trainings richten wir generell auf die individuellen Kundenanforderungen aus.

3.6 Zugriffssicherheit für autorisierte Anwender

VPSC (Virtual Protected Secure Communication)



Die Authentifizierung erfolgt in drei Schritten:

1. Der autorisierte Anwender ist im Besitz des vorkonfigurierten SAY**TRUST**-Sticks und kennt seine Remote Access PIN.
2. Schritt: Die Identität des Anwenders wird mittels seines Fingerabdrucks geprüft. Der Zugriff auf Daten auf dem SAY**TRUST** Client ist zunächst hardwareverschlüsselt blockiert. Dies gilt selbstverständlich auch für die Biometriemerkmale. Erst nach erfolgreicher Eingabe des Fingerabdrucks wird automatisch das Client-Menü gestartet. Dieser Vorgang kann wahlweise durch eine zusätzliche PIN-Abfrage gesichert werden.
3. Schritt: Herstellung einer Remote-Verbindung mit dem Business-Netzwerk. Dazu wird erst die Remote Access PIN abgefragt. Die Komplexität dieser PIN kann serverseitig eingestellt werden. Anschließend wird das User-Zertifikat überprüft und aktualisiert. Damit „kennt" der Client seine aktuellen Berechtigungen.
4. Nach dieser letzten Authentifizierung werden die Berechtigungen des Users bereits vom Client aus geprüft und entsprechend der eingerichteten Policies auf Applikationsebene getunnelt. Dabei wird für jede Anwendung eine gesonderte Kommunikation innerhalb des SAY**TRUST** VPSC Tunnels direkt vom Arbeitsspeicher aus aufgebaut. Der Tunnel ist somit für jedwede Schadsoftware gesperrt. Es können ausschließlich berechtigte Anwendungen mit dem Remote-Netzwerk kommunizieren.
5. Der SAY**TRUST** Client nimmt eine eindeutige Authentifizierung vor.
6. Der gesamte Datenbestand liegt hinter dem SAY**TRUST** Server und ist deshalb für Unberechtigte nicht erreichbar.

4. Bestandteile der SAYFUSE Infrastructure Appliance

Die Produkte aus der SAYTEC Solutions-Konzeptreihe stellen die gesamte IT-Infrastruktur für Unternehmen bereit und ermöglichen eine signifikante Reduzierung der IT-Komplexität bei gleichzeitiger Erhöhung der Sicherheit und Verfügbarkeit. Durch redundante Bereitstellung der Serversysteme, bis hin zum Cluster für die gesamte IT-Infrastruktur, wird auch die Verfügbarkeit in Katastrophenfällen gewährleistet.

Grundsätzlich wird sichergestellt, dass ausschließlich berechtigte Personen Zugang zu sensiblen Daten haben. Dazu ist ein eindeutiges Authentifizierungsverfahren notwendig. Die Authentifizierungsdaten dürfen zu keinem Zeitpunkt in falsche Hände gelangen.

SAY**TRUST** Access stellt dies zu jedem Zeitpunkt der Datenübertragung sicher. Dadurch wird die gesamte Kommunikation innerhalb des Netzwerkes und auch von außen in das Unternehmensnetzwerk abhörsicher.

4.1 Lieferumfang der Infrastructure IT-Infrastruktur Appliance

- Plattform für die gesamte IT-Netzwerk-Infrastruktur
- Plattform für Sicherung, Wiederherstellung und Auslagerung
- Hochsichere SAY**TRUST**-VPSC-Kommunikationsplattform
- Peripherie
- Installations Packet
- Service & Support Sorglos Packet

4.1.1 Eine Appliance für die gesamte Netzwerk-Infrastruktur

a. Virtuelle Server wie Domaincontroller, Applikations-, File-, Datenbankserver, … (ein Server im Lieferumfang)
b. Server-Storage
c. Daten-Storage
d. Virtualisierung-Hypervisor
e. Virtuelle Arbeitsplätze (optional)

4.1.2 Backup und Restore Plattform: Eine Appliance für die Sicherung, Wiederherstellung & Auslagerung der Daten und Serversysteme

a. Backupserver
b. Media-Handling Software
c. Backup Software
d. Backup- oder Dedup-Storage
e. Sechs Backup-Laufwerke für Sicherung, Medienbruch und Auslagerung
f. Backupmedien
g. Backup-Library-System

4.1.3 Hochsichere Kommunikationsplattform: Integriertes SAY**TRUST** Access VPSC Kommunikationssystem für die interne und externe Kommunikation

a. SAY**TRUST** Access VPSC Server
b. Fünf SAY**TRUST** Remote Access Clients
c. Fünf SAY**TRUST** Internal Network Clients für die hochsichere Abschottung
d. Secure Cloud für Mitarbeiter
e. Secure File-Transfer Modul für die sichere Datenübertragung

4.1.4 Peripherie im Lieferumfang

a. Ausziehbares Rack-Mount Keyboard (Monitor, Tastatur, Touchpad)
b. Patchkabel für Verkabelung
c. Thin-Client-Rechner (optional)
d. saySNOW-Rechner (optional)

4.1.5 SAYTEC Solutions - Installations-Paket

a. Anlieferung
b. Einbau, Installation & Konfiguration
c. Einweisung

4.1.6 Service & Support

a. Software-Updates der verwendeten SAYTEC-Produkte
b. Hard- und Software-Support während der Laufzeit
c. Regelmäßige Wartung
d. Reparatur & Austauschservice
e. Ersatzgerät während der Reparatur
f. Die Reaktionszeit für den Remotesupport ist vom jeweiligen Service-Vertrag abhängig in der Regel 3 – 4 Stunden
g. Austauschservice am nächsten Business-Day

4.1.7 Erweiterungsmöglichkeiten

a. SAY**TRUST** Share–Cloud–Module
b. SAY**TRUST** VoIP (abhörsichere Sprachkommunikation)
c. Personal zu Personal
d. Unternehmen zu Kunden
e. Kunden zu Unternehmen
f. SAY**FUSE** NVR (Videoüberwachung)

4.2 Weitere Vorteile

4.2.1 Kosteneffizienz

Das SAY**FUSE** VM Backup stellt für Unternehmen einen kostengünstigen Einstieg in die Server-Virtualisierung in einer einzigen Appliance bereit und beinhaltet dabei sogar ein komplettes Datensicherungs-System. Die Anschaffungs- und Betriebskosten wer-den somit deutlich reduziert.

4.2.2 Skalierbarkeit

Mit sechs bis zu 32 Stellplätzen für Server RAID und einer Kapazität von 5 TB bis 1024 TB können bereits mehrere Server virtualisiert werden. Zusätzlich steht ein Datensicherungsvolumen bis zu einer maximalen Auslagerung von 250 TB zur Verfügung. Die Gesamtkapazität für die Datensicherung und Storage kann durch das optional erhältliche Modul SAY**FUSE** CEM erhöht werden.

4.2.3 Automatisierung

Im Standardlieferumfang ist die Software sayCONTROL zur Steuerung der Backup-Medien-Laufwerke bereits enthalten. Als Betriebssysteme für die Virtualisierung sind Microsoft Hyper-V, Citrix XenServer oder VMware vSphere™ erhältlich.

Das SAY**FUSE** Backup kann mit allen am Markt erhältlichen Backup Software-Lösungen verwendet werden. Empfohlen wird SEP sesam, das in speziellen OEM-Bundles für SAY**FUSE** mit erweiterter Funktionalität angeboten wird.

4.2.4 Peformance

Das SAY**FUSE** Backup vereint die Vorteile des Mediahandlings von Tape Library Systemen mit denen von festplattenbasierten Sicherungslösungen. Backup und Restore werden gegenüber bandbasierten Lösungen signifikant beschleunigt, so dass Unternehmen mehr Daten innerhalb des verfügbaren Backup-Fensters sichern und nach einem Datenverlust schneller wieder produktiv arbeiten können. Die Anbindung an das Netzwerk erfolgt standardmäßig über 2 x 10 Gbit/s und kann optional auf weitere 10 Gbit/s erweitert werden.

4.2.5 Flexibilität

Unterschiedliche Mediengrößen (Kapazitäten) können sowohl für den Server-RAID als auch für die Datensicherung im Mischbetrieb genutzt werden. Im Datensicherungsbetrieb können parallele Backups erfolgen. Backup-Medien können zu Pools zusammengefasst werden.

4.2.6 Sicherheit

Unterschiedliche Backup-Medien können - wie Tapes - einfach aus dem System entnommen und z.B. in einem Bank-Safe aufbewahrt werden.