KONICA MINOLTA

Ürün Tanıtımı
Dijital Doktor Araçları İçin Gelişmiş Güvenlik Kılavuzu

- Durum: 04/ 2016
- Sürüm: 2.6

Giving Shape to Ideas

KONICA MINOLTA OPTIMIZED PRINT SERVICES™

İçindekiler

KONICA MINOLTA OPTIMIZED PRINT SERVICES ™

Konica Minolta Güvenlik İlkeleri

1. **Konica Minolta tüm ağ ortamlarında güvenle kullanılabilecek yazılım ürünleri geliştirmek için sürekli çalışmaktadır. "Dijital Doktor" hizmetleri yalnızca bir yazdırma ortamının yönetimi için gereken cihaz servis verilerini toplar. Asla kişisel bilgileri, kullanıcı bilgilerini, yazdırma verilerini ya da yazdırma işi bilgilerini toplamaz.**

2. **Konica Minolta MFP'de saklanan bilgiler**

   Tüm Konica Minolta marka çok işlevli ürünlerde (MFP) veri depolamak için iki çeşit bellek ve bir hard disk sürücüsü mevcuttur. (Hard disk sürücüsü bazı ürünlerde opsiyoneldir.)

   2.1.1. Makine belleği

   Makine belleği (NVRAM) MFP ile ilgili tüm bilgileri saklar (makine ayarı verileri, sayaç bilgileri ve sorun bilgileri gibi) ve bunları güç kesildikten sonra bile bellekte tutar.

   2.1.2. Görüntü belleği

   Bu görüntü belleği (SDRAM) görüntü işleme amaçlı belge ve görüntü verileri ile ilgili bilgileri geçici olarak saklar.

   2.1.3. Hard disk sürücüsü

   Hard disk belge ve görüntü verilerini görüntü işlendikten sonra bir dosya formatında saklar.

3. **Konica Minolta MFP'leri HDD üzerinde depolanan verilerin yönetilmesi için çeşitli güvenlik seçenekleri sunmaktadır. HDD üzerinde depolanan verilerle ilgili güvenlik ayarları hakkında daha fazla bilgi için belgenin Güvenliğin Temelleri belgesine göz atın.**

KONICA MINOLTA OPTIMIZED PRINT SERVICES™

CS Remote Care System

1. Genel

Konica Minolta CSRC sistemi yalnızca yukarıda belirtilen makine belleğindeki verileri çeker ve görüntü belleği veya hard disk sürücüsünde bulunan verilere erişemez.

2. CSRC sisteminin aldığı bilgiler

- **MFP bilgileri**
  Firma yazılımı (ROM) sürüm bilgisi, MFP kimlik bilgileri ve yapılandırma bilgileri

- **MFP kullanım durumunu belirten bilgiler**
  Çeşitli ayar bilgileri

- **MFP durumunu belirten bilgiler**
  İkazlar (toner ekleyin, görüntüleme ünitesini değiştirin, vb.), hata kodları, düzenli bakım bilgileri, kağıt sıkışması veya teknik geçmiş bilgileri gibi çeşitli MFP bilgileri.

- **MFP işlemleri ile ilgili çeşitli ayar değerleri**
  Çeşitli sayaç bilgileri
  Toplam sayaç değerleri, kağıt ölçülerine göre sayı, parça sayaçları, sıkışma sayacı

Not:

Aşağıdaki kişisel bilgiler alınmaz

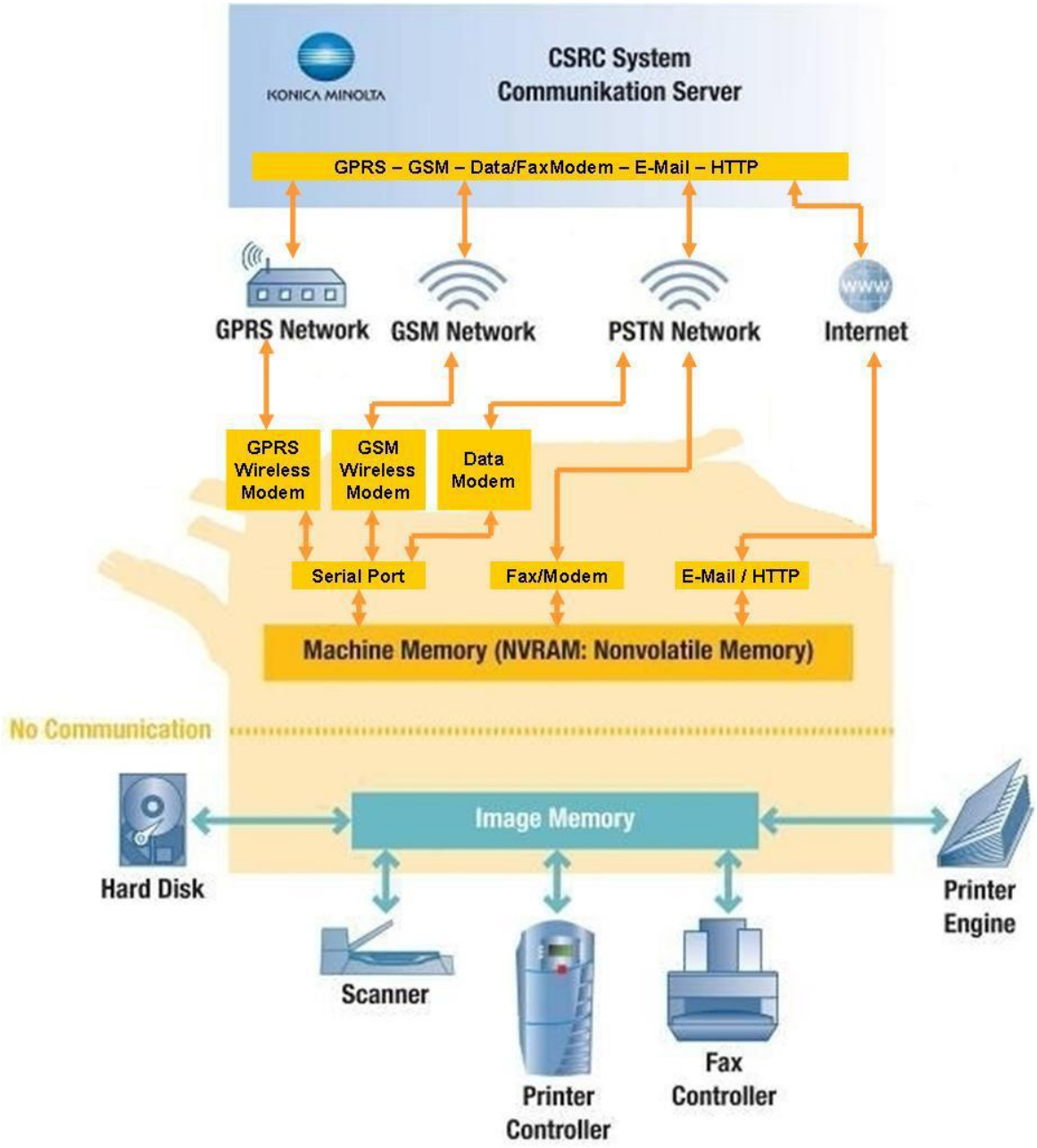
- Kullanıcı doğrulama işlevi etkinleştirilmişse: kullanıcı bilgileri ve kullanıcıların sayaç bilgileri alınmaz.

- FAKS/Tarama işlevleri için tek dokunuşla işlem işlevi gibi çeşitli MFP işlevleri için kaydedilen adres bilgileri.

- Diğer kayıt bilgileri, ör. kayıtlı belgeler ve bu belgelerle ilgili bilgiler.

KONICA MINOLTA OPTIMIZED PRINT SERVICES ™

3. CSRC Sistem İletişim Sunucusu



4. CSRC sistemi ile Konica Minolta MFP arasındaki haberleşme

4,1. Haberleşme süreci

CSRC yalnızca aşağıdaki iki durumdan biri gerçekleştiğinde MFP ile iletişime geçer:

MFP Bilgileri

- Sistem kullanıcısı haberleşme talep ettiğinde.
- Sistemin rutin, önceden belirlenmiş haberleşme saati geldiğinde.

MFP haberleşmeyi başlatır

- MFP bir sorun tespit ettiğinde veya alarm verdiğinde. (Her modelin önceden belirlenmiş hata çeşitleri mevcuttur. Bunlar CSRC sistemine otomatik olarak bildirilir.)

MFP'den alınan sorunlar ve uyarılar ciddiyetlerine göre çeşitli şekillerde yönetilirler. Biz bu "çağrıları" aşağıda görülen dört kategoriye ayırıyoruz:

Yüksek: Bu uyarılar bir saha teknisyeninin alanda müdahale etmesi gerektiği anlamına gelir. Bu niteliğe uyan sorunlar kaydedilir ve saha teknisyenine otomatik olarak gönderilir. Bu da saha teknisyenleri PDA'sına bilgi veren Konica-Minolta bölge yönetim sistemi kullanılarak sağlanır. Saha teknisyeni sorun CSRC Yönetim sistemi tarafından alındıktan sonra birkaç saniye içinde bilgilendirilir.

Orta: Bunlar müşteri ile doğrudan görüşerek çözülebilen sorunlardır. Bu niteliğe uyan sorunlar servis yönetimi sisteminde kayıt altına alınır ve yerel servis yöneticisine sunulur. Yerel servis yöneticisi de müşteri ile irtibata geçer. Sorunun daha ciddi olduğu anlaşılırsa ve bir servis müdahalesi gerekiyorsa, servis yöneticisi saha teknisyenlerini görevlendiren bölge yönetim sistemini kullanarak müdahaleyi organize edecektir.

Düşük: Bu sorunlar tek başlarına önem teşkil etmese de üst üste geldiklerinde sıkıntılara sebep olabilirler. Bunlar sayılır ve belirli bir süre zarfında belirli bir sınırı aşarlarsa servis yöneticisine iletilirler. Servis yöneticisi de müşteri ile irtibata geçer.

Uyarılar: Bu mesajlar cihazda toner, kağıt, zımba, vb. kalmadığını bildirir. Toner mesajını aldığımızda SUPPLY (TEDARİK) hizmetimizi etkinleştiririz.

Sistemin hata çağrısını kabul etmesi ve sahada müdahalenin gerekmesi durumunda, müşteriye ayrıntıları, hata numarasını, hata kabul saatini, sorunun açıklamasını, vb. içeren bir e-posta/faks gönderilir.

4.2. Haberleşme yöntemi

CSRC sistemi MFP ile haberleşme için aşağıdaki, ön ayarlı yöntemlerden birini kullanır.

1) Veri haberleşmesi (mobil ağ bağlantısı bulunan kablosuz modem ya da PSTN'li veri modemi).

CSRC sistemini MFP'ye (ITU-T V.34/V.32.to/V.32- ile uyumlu) bir modem bağlar. Bağlantı kurulduktan sonra, CSRC sistemi veri alışverişini CSRC orijinal protokolü ile yapar. Orijinal CSRC protokolü kullanıldığı için izinsiz uzaktan erişim girişimleri reddedilir.

2) Faksla haberleşme (faks modemi ve PSTN kullanarak).

Tüm veri haberleşme yöntemleri arasında en güveniliri FAKS bağlantılarıdır. Veri ya MFP'nin yönetim sistemini araması ya da tam tersi şekilde gönderilir/alınır.
Gönderilerde faks tonları kullanılır. Cihazlar birbirlerini aradıklarında, cihazlar kendilerini kurulum esnasında girilen parolalarla tanımlar.
Yönetim sistemi kaydedilmemiş bir sistemden çağrı alırsa, işlem iptal edilir. Benzer şekilde, MFP yönetim platformunun çağrısını ancak başarılı parola alışverişi sonrasında kabul edecektir. Yönetim sisteminin aranıp veri alınması mümkün değildir. Fotokopi makinesini arayıp da müşterinin ofisindeki bağlı diğer cihazlara bağlanmak da mümkün değildir. Yalnızca belirli MFP'lerin sayaç bilgileri alınabilmektedir.
CSRC sistemini MFP'ye (ITU-T T.30- ile uyumlu) bir modem bağlar. Bağlantı kurulduktan sonra, CSRC sistemi veri alışverişini CSRC orijinal protokolü ile yapar. Standart G3 FAKS protokolünün yerine orijinal protokolün kullanılması veri sahteciliğini önler.

3) E-posta ile haberleşme

E-postalar POP ile alınır ve SMTP ile gönderilir. E-posta gönderirken MFP ağa giriş yapmaz, bu yüzden e-postanın müşterinin ağını terk edebilmesini sağlayabilmek için posta iletim hizmetine [SMTP] fotokopi makinesinin IP adresinin "güvenilir" yani güvenli olduğunun ve postaların müşteri alanından çıkmasına izin vermesinin söylenmesi gerekmektedir. E-posta almak için fotokopi makinesi POP hizmetine bağlanır ve bu hesaptan e-posta almak için kendini tanıtır. Bu sisteme giriş işlemi düz metin formatında gerçekleştirilir. Bazı müşteriler MFP ile POP ve SMTP ile harici sunucu arasında bağlantıya izin vermektedir; bu durumlarda bizim (Konica Minolta) uzaktan posta sunucu IP adresimiz kullanılabilir. Diğer müşteriler POP e-postalarının uzaktan posta sunucularımızdan alındığı ve SMTP postalarının müşterinin kendi ağı üzerinden gönderildiği karma sistemler kullanmaktadır. Fotokopi makinesindeki görüntülerin alınmasının ya da müşterinin ağı üzerindeki başka bir cihaza bağlanmanın mümkün olmadığı unutulmamalıdır.

Veri hırsızlığını, veriler üzerinde oynama yapılmasını ya da müşteri ağına izinsiz erişimi ve virüs ya da Trojan (Truva Atı) gibi zararlıların sızmasını önlemek için aşağıdaki güvenlik önlemleri uygulanmıştır. Orijinal CSRC protokolünün kullanılması sahte e-postaları da önlemektedir.

Veriler düz metin formatındaki e-posta ekleri şeklinde gönderilir, fakat şifreleme ayarları etkinleştirilmişse metin şifrelenebilir. Şifrelenmiş veriler sahte bilgiler ile başka birine ulaştırılsa bile çözülemeyecektir.

MFP e-postaları yalnızca belirli bir format şeklinde alabilmektedir: konu, parola ve ek dosyalar (ek sayısı, dosya formatı ve uzantı). Bu formata uymayan e-postalar silinir. MFP çalıştırılabilir dosyaları desteklemediği için virüsler .exe (veya betik biçimi dilleri) dosyaları ile müşteri ağına sızamaz. MFP işletim sistemi Windows veya diğer ofis İS'lerinden farklıdır; virüsler yayılamayacaktır. MFP tarafından oluşturulan yanıt e-postası alınan e-postayı yanıtlamaz. Bunun yerine, sistem kurulum esnasında kaydedilen barındırma adresine yeni bir e-posta gönderir. Barındırma adresi ve parolası uzaktan değiştirilemez. Bu da yazılım MFP üzerinden yapılandırılmadığı müddetçe başka bir platforma bağlanmanın mümkün olmadığını anlamına gelmektedir.

Tavsiyeler
Müşteri ortamında filtreleme yazılımı kullanılıyorsa:

- MFP'ye gelen e-postayı gönderenin kayıtlı barındırma adresinden olmaması durumunda e-postanın silinmesi için bir kural belirlenebilir. (Örnekler: istenmeyen postalar veya diğer cihazlardan izinsiz erişim)

- MFP'den gönderilen e-postanın alıcısının kayıtlı barındırma adresi olmaması durumunda e-postanın silinmesi için bir kural da belirlenebilir.

4) Siemens TC65 ile GPRS

Siemens TC65 MFP'ye RS232 arayüzü üzerinden bağlanan standart bir GPRS modemidir. TC65 modemlerde M2MGate adında bir Java yazılımı kullanılmaktadır:

M2MGate MFP için bir CSD modemi emüle edecek ve MFP bir "AT" Komutu gönderdiğinde "OK" yanıtı verecektir. Bu yazılım MFP'yi arayabilir, gelen veri çağrısını simüle eder ve KM seri haberleşme protokolünü gerçekleştirir. MFP'nin seri portu yalnızca CSRC orijinal protokolü kabul ettiği için izinsiz uzaktan erişimler engellenir. Modem Veri-Taleplerini komut tokeni dizgesi olarak alacak ve MFP haberleşmesini her bir komut tokenini MFP'ye ayrı ayrı göndererek başlatacaktır. Bir komut tokeninde sintaks hatası olması durumunda, yalnızca ilgili sonuç silinecektir. Tüm geçerli talepler talep eden sunucuya tek bir mesaj halinde geri gönderilecektir. MFP'den alınan Alarmlar ve Kurulumlar M2MGate ile sunucuya iletilecektir. Kurulum esnasında program cihazın sunucu tarafında tanınıp tanınmadığını kontrol edecektir. Buna ek olarak sorun gidermek ve yazılımı OTAP (Havadan İletim Prosedürü) üzerinden güncellemek için iki hizmet mevcuttur. Yazılım cascade (kademeli) sunucu ile olan bağlantıyı açık tutmaya çalışır. Bu da alarm veya mesaj gibi olağan trafik gerçekleşmediğinde bağlantının düzenli aralıklarla kontrol edileceği anlamına gelmektedir.

Güvenliği arttırmak için aşağıdaki güvenlik özellikleri mevcuttur

- SIM-PIN kullanımı mümkündür
- SSL şifreleme mümkündür (TC65 ile cascade sunucu arasında)
- Sunucu sertifikasının TC65'te müdahale korumalı bir şekilde depolanması
  - Sunucunun SSL ile doğrulanması mümkün
  - Yalnızca imzalı Midletlerin çalıştırılması mümkün
- TC65 üzerindeki AT İşleyicisine güvenli kanal üzerinden erişim
  - Parola ve parametre değişikliği
  - Kapsamlı sorun giderme
  - SMS olmadan OTAP hazırlığı mümkün

5) http(s) Transfer yöntemi

CSRC http bağlantısı cihaz ile CSRC sunucusu arasında WebDAV sunucusu üzerinden yeni bir bağlantı yöntemi sağlar. http bağlantısı http ve https destekler. https kullanmanız önerilir. BEU merkezi sunucu ortamı daima https kullanır. Cihaz ve CSRC sunucusu gerekli dosyaları yüklemek ve indirmek için WebDAV sunucusundaki bir klasöre düzenli olarak erişim sağlar. Haberleşme için bir http(s) portu (varsayılan port http için 80 ve https için 443'tür) kullanılacaktır. http protokolünün güvenlik duvarında yalnızca içeriden dışarıya bağlantılar için etkinleştirilmesi gerekmektedir. Cihaz WebDAV sunucusu ile haberleşmeyi başlatır. Güvenlik duvarında dışarıdan içeriye gelen bağlantılar için bir ayar yapılması gerekmez. Cihaz dış dünyadan tamamen gizlenmek için bir vekil sunucu kullanacak şekilde de ayarlanabilir.

Dosya formatı e-posta üzerinden haberleşme ile aynıdır. Dosya veri şifrelemesi de e-posta haberleşmesi ile aynı tekniğe göre yapılabilmektedir. Ancak, HEART BEAT dosyası şifrelenemez. E-posta ile haberleşmeye benzer şekilde, iki bağlantı çeşidi mevcuttur: tek yönlü (simplex) ve interaktif (duplex). Tek yönlü bağlantılarda tüm haberleşmeleri yalnızca cihaz başlatır.

HEART BEAT işlevi cihazın WebDAV sunucusuna düzenli aralıklarla (varsayılan olarak her 30 dakikada bir) erişmesini sağlar ve aşağıdaki dosyayı belirtilen klasöre kaydeder. Bu işlev devre dışı bırakılabilir.

Örnek: HEART BEAT (HB) dosyasının ayrıntıları

SD, <durum>, <toplam sayaç>
- **SD** (zorunlu) : **S**aat **D**ilimi ayarı yapılmalıdır
  - **Durum** (isteğe bağlı): 0 - 7
    0: Belirtilmemiş
  1: Güç AÇIK
  2: Güç KAPALI
  3: Boşta
  4: İş başlatıldı
  5: İş tamamlandı
  6: Sıkışma sebebiyle durduruldu
  7: Sıkışma giderildi
  Bu tanımın üründen ürüne farklılık gösterebileceğini unutmayın. - **Toplam sayaç** (isteğe bağlı)

WeBDAV sunucusuna HB erişimi gerçekleştiğinde sunucu HB dosyasını kaydeder ve bu cihaz için bir CSRC komut talebi olup olmadığını kontrol eder. Bir CSRC komut talebi varsa, talep MFP'ye indirilir ve ilgili CSRC komutları işlenir. HB işlevi kapatıldığında CSRC komut talebi dosyası WebDAV sunucusundan yalnızca MFP veri (ilk bağlantı, zamanı belirlenmiş bağlantı, ikaz bağlantısı, vb.) gönderiyorsa alınabilir.

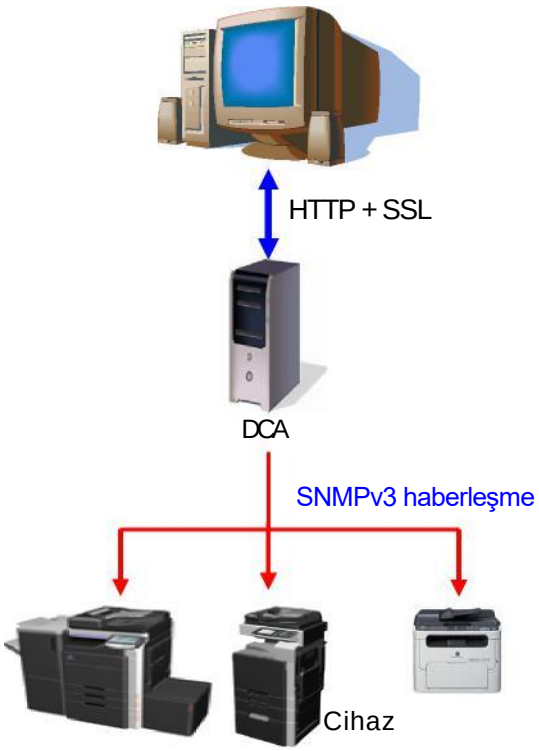
CSRC iletişim sunucusu WebDAV sunucusuna http(s) üzerinden bağlanır ve yönetilen cihazları için bir talep dosyası olup olmadığını sık sık (varsayılan olarak her dakika) kontrol eder. Komut dosyası olması durumunda ilgili dosya haberleşme sunucusuna indirilir ve işlenir.

6) CSRC DCA

DCA (Cihaz Toplama Programı) cihazlarla haberleşme yöntemi için SNMPv1 ve SNMPv3 haberleşme protokollerini kullanmaktadır.
SNMPv1 haberleşme protokolünde düz metin ağ yolunu izler ve ortamda paketlerin dışarıdan ele geçirilmesi riski mevcutsa veriler iletim esnasında çalınabilir.
SNMPv1'deki tek doğrulama etkeni olan "topluluk adı" da aynı zamanda sızdırıldığı için, sızdırılan "topluluk adı" ile yönetilen cihazın MIB'sinde saklanan tüm veriler de izinsiz erişime açık olur.
SNMPv3'te ise SNMPv1'deki "topluluk adı"na denk gelen "kullanıcı adı"na ek olarak, cihaz erişiminin korumasını arttırmak için bir doğrulama mekanizması eklenmiştir. Haberleşme yolundan geçen verilerin tamamı şifrelenir; bu yüzden şifreleme sistemi/şifreleme anahtarı bilinmediğinde veri hırsızlığı zorlaşır.

DCA ile CSRC barındırma sistemi arasındaki haberleşme HTTP protokolünde SSL kullanılarak şifrelenir. Ayrıca DCA'ya benzersiz bir kimlik atanır ve veri aktarımı her haberleşmede kimlik kontrolü sonrasında gerçekleştirilir. Haberleşme kimliği eşleşmezse veri gönderilmez.

CSRC barındırma sistemi



Şekil 9-4

CS Uzaktan Analiz

CSRA (**CS Uzaktan Analiz**) düzenli aralıklarla MFP'lerin sensör verileri gibi çeşitli verileri toplayan, arızaları analiz ve tahmin eden ve toplanan verilere göre parçaların ömrünü tahmin eden bir sistemdir. Sorunun uzaktan analiz edilmesi servis temsilcisinin ilgili müdahaleyi müşteriyi ziyaret etmeden önce planlayabilmesini ve bakım işlemini herhangi bir aksaklık olmadan gerçekleştirebilmesini sağlar.
CSRA ile toplanan veriler sensör verisi değerleri gibi mekanik kontrol bilgilerinden oluşur ve kişisel bilgiler ve/veya şahsi bilgiler içermez. CSRA işlevlerinin etkinleştirilebilmesi için Saha servis temsilcisinin müdahalesi gerekmektedir.

1. HTTP haberleşmelerinde güvenlik

CSRA ile haberleşmenin başlatılabilmesi için bir CSRC haberleşmesi başlatılmalıdır. MFP veri göndermeden önce CSRC sunucusunu doğrular.

- Simplex haberleşmesi

CSRA MFP'den alınan CSRA Verilerini belirlenen sunucuya düzenli aralıklarla göndermek için https simplex haberleşmesini (Cihaz □ CSRA Sitemi/CSRA atanmış haberleşmesi - CSRC ile ilgili değildir) kullanır. Harici sunuculardan gelen erişim taleplerine izin verme işlevine sahip değildir.

- Gönderilen verilerin şifrelenmesi

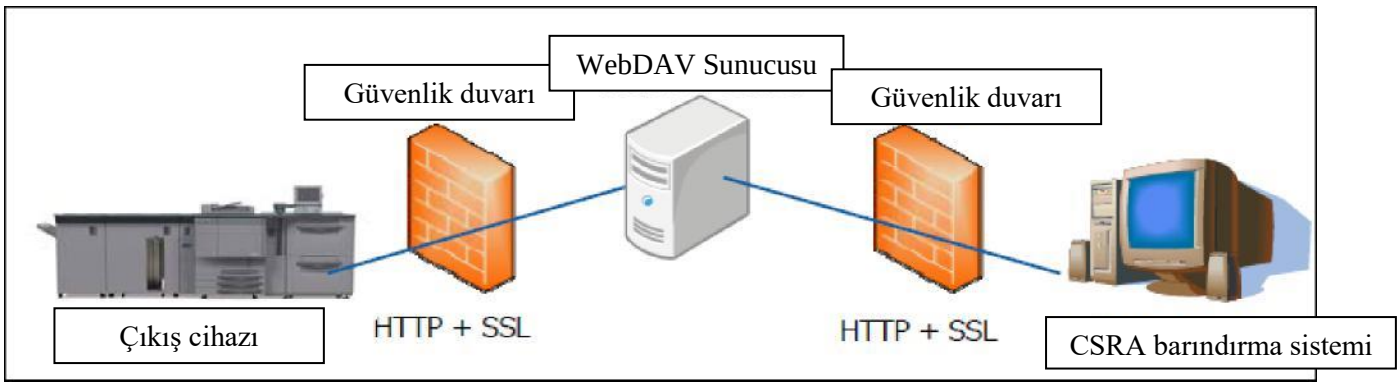
HTTP haberleşmelerinde SSL mevcuttur (HTTPS). CSRA gönderen cihaz ile WebDAV sunucusu arasında ve WebDAV sunucusu ile CSRC host sistemi arasında iki yönlü olarak gönderilen tüm verileri şifreler.

- HTTP protokolünün çeşitli güvenlik işlevleri uyumludur

Ortamından bağımsız olarak HTTP protokolü doğrulama, vekil bağlantı ve SSL gibi çeşitli güvenlik işlevlerinden faydalanabilir.

SSL açık anahtarlar, özel anahtarlar, dijital sertifikalar ve özet işlevleri gibi güvenlik teknolojilerinden faydalanarak verilerin bozulmasını, tahrif edilmesini ve/veya sahtelerinin gönderilmesini önler.

Bu güvenlik işlevleri uzaktan kontrol merkezinin müşterilere her ofis ortamına uygun güvenlik önlemleri sunabilmesini sağlar.



KONICA MINOLTA OPTIMIZED PRINT SERVICES ™

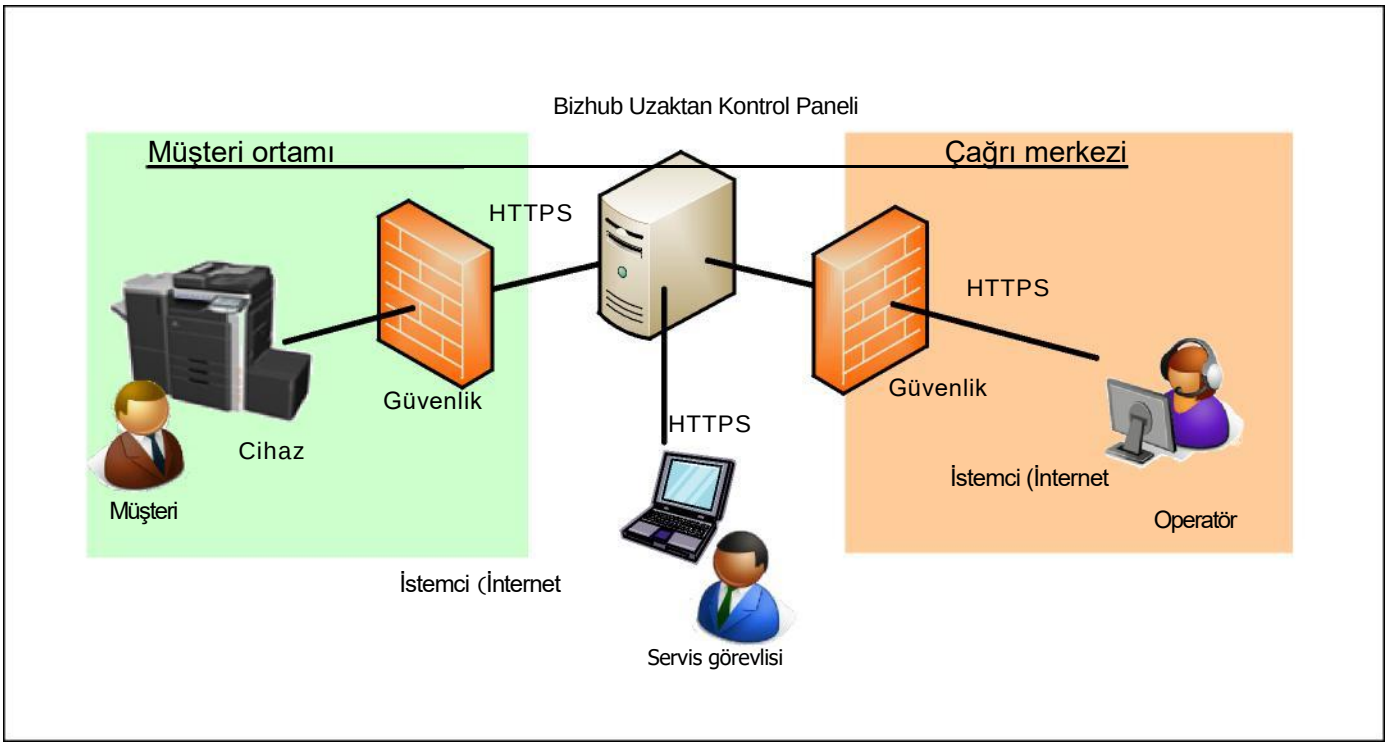
Bizhub Uzaktan Kontrol Paneli

1. Haberleşme, Bağlantı tetikleyicisi
   Bizhub Uzaktan Kontrol Paneli şifre anahtarı olmadan HTTP bağlantısı gerçekleştiremez. Bağlantılar SSL ile şifrelenip HTTPS üzerinden gerçekleştirilir.
   Buna ek olarak, bizhub Uzaktan Kontrol Paneli Sunucusu tarafından cihazlara bağlantı devre dışıdır. Bağlantı yalnızca cihazlardan yapılabildiği için müşteri güvenliği güvence altına alınır.

2. Doğrulama
   Güvenilir üçüncü şahıs CA (Sertifika Yetkilisi) tarafından cihazlar ve bizhub Uzaktan Kontrol Paneli Sunucusu için düzenlenen sertifika sayesinde daha da güvenli bir haberleşme sağlanmıştır.

3. Erişim Kodu
   bizhub Uzaktan Kontrol Paneli Sunucusunu birden fazla cihaz ve birden fazla kullanıcı (istemci) kullanabilir. Kullanıcı cihaz listesinden bağlanacakları cihazı seçer ve 4 haneli Erişim Kodunu girer. Cihaz panelinde görüntülenen doğrulanmış 4 haneli Erişim Kodu müşteri (servis görevlisi ile operatör) tarafından önceden yetkilendirilmiş olan istemciye gönderilir.

4. Denetim kaydı
   bizhub Uzaktan Kontrol Paneli Sunucusuna bir cihaz bağlandığı zaman, istemcinin (kullanıcı) cihazı uzaktan kullanması ve çıkış yapması ile ilgili kayıtlar tutulur. Admin bizhub Uzaktan Kontrol Paneline erişimleri bu kaydı izleyerek takip edebilir.



Printfleet

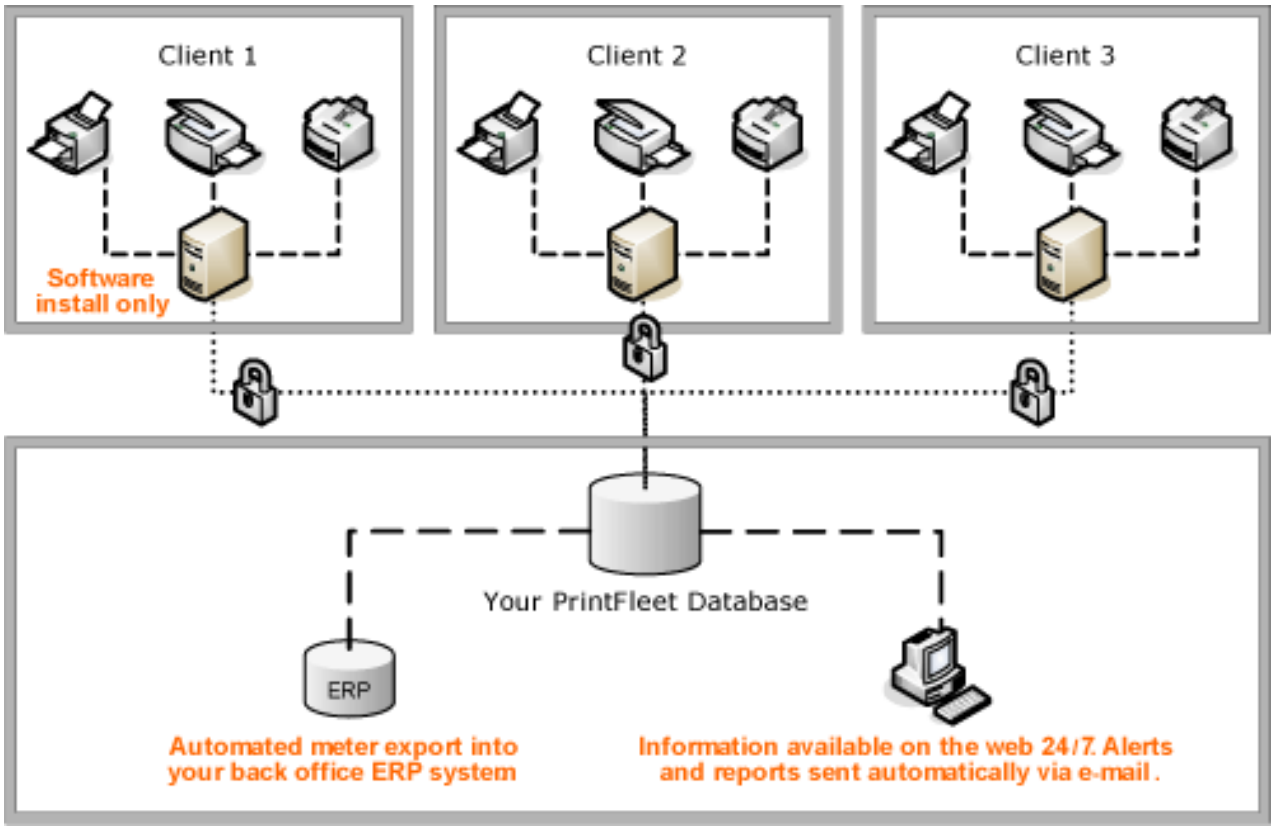
1. Genel

Printfleet Konica Minolta ürünlerine ek olarak diğer üreticilerin ürünlerini de destekler. Printfleet sistemi yalnızca yukarıda belirtilen makine belleğindeki verileri çeker ve görüntü belleği veya hard disk sürücüsünde bulunan verilere erişemez. Bu, Konica Minolta CSRC sistemi ile aynıdır.

2. Printfleet sisteminin aldığı bilgiler

- IP adresi (gizlenebilir)
- Cihaz açıklaması
- Seri Numarası
- Ölçüm Değerleri
- Monokrom veya renkli belirleme
- LCD değerleri
- Cihaz durumu
- Hata kodları
- Toner seviyesi
- Toner kartuşu seri numarası
- Bakım kiti sevisi
- Toner dışı tedarik seviyeleri
- Varlık numarası
- Konum
- MAC Adresi
- Üretici
- Firma yazılımı
- Diğer (makineye özel

3. **Printfleet sistem konfigürasyonu**



4. Printfleet sistemi ile Cihaz arasındaki haberleşme

4,1. Haberleşme süreci

OPS Veri Toplama Programı (DCA) ağa bağlı görüntüleme cihazları veya yerel bağlı yazıcıların değerlerini toplamak için kurulan bir yazılım uygulamasıdır (bunun için programın kurulu ve çalışıyor olması gerekir). DCA bir Windows hizmeti (ya da isteğe göre planlanmış bir görev) olarak çalışır ve bu sayede haftada 7 gün ve günde 24 saat etkin kalabilir.

Özellikle de aşağıdaki durumların geçerli olması halinde, müşteri ortamları için birden fazla DCA kurulumu yapılabilir

- çok alanlı kurulumlar
- düşük bant genişliği bulunan WAN'ler
- ayrı ağlar
- çok büyük filolar (>2.000 yazıcı)

Bu durumda, ikili kapsama alanları (2 DCA'nın aynı makinenin verilerini toplaması) verilerin gönderildiği veritabanı tarafından çözülür.

Ağ gereksinimleri:

- TCP/IP yapılandırması
- HTTPS Portu 443, DCA'dan merkezi veritabanına aktarım mümkün
- internete yalnızca tek yönlü bağlantı
- Cihaz taraması için UDP Portu 161 SNMP v1 Dahili ağ

Sistem gereksinimleri:

- Donanım: 7/24 çalışan atanmamış sunucu. Sunucu mevcut değilse, DCA bir masaüstü bilgisayar sistemine de kurulabilir (7/24)
  Güvenilir Donanım
- İşletim sistemi: Windows 7 / 8, Windows Server 2008 / 2012
- Ağ kartı: 100Mbit veya üstü, sistemde yalnızca bir etkin ağ kartı olmalıdır
- CPU 1 GHz veya üstü
- Ram: 512 MB veya üstü
- Microsoft .NET Framework 2.0 SP2, ya da Microsoft .Net Framework 3.5 SP1, veya üstü (Client Profile sürümü hariç)
- İnternete bağlanabilen bir tarayıcı
- Virtual Machine (Sanal Makine) Desteği: Microsoft Virtual Server 2005, VMWare GSX

4,2. Haberleşme yöntemi

DCA müşterinin özel (LAN/WAN) ağında belirli aralıklarda görüntüleme cihazı verilerini (SNMP, ICMP ve HTTP) toplar. DCA bu verileri HTTPS-Protokolü ile korunan merkezi veritabanına gönderir. Verilerin HTTPS ile gönderilmesi prosedürü bir kullanıcının bilgisayarında standart bir internet tarayıcısı ile bir HTTPS internet sayfasını açması ile aynıdır.

Bu yüzden:

- güvenlik duvarında özel portların açılması gerekmez
- DCA'da yalnızca, varsa, vekil sunucu ayarlarının yapılması gerekir

DCA'dan veritabanına yapılan bağlantı yalnızca dışa doğrudur. Bu şekilde ayarlanmışsa, DCA'ya gelen bağlantı yoktur.

(Not: DCA'da "Akıllı Güncelleme" etkinleştirilmişse sunucuya her bağlandığında yeni yazılım sürümü olup olmadığını sorar. Yeni yazılım sürümü DCA bağlantıyı başlattıktan sonra indirilebilir.)

HTTPS iletim yöntemi port 443 üzerinden SSL şifreleme kullanmaktadır. Merkezi internet sunucusuna bir VeriSign SSL sertifikası kurulmuştur https://ops.konicaminolta.eu. Yerel DCA ile kurulan bağlantı yalnızca belirli bir hedef üzerine sınırlanabilir.

Veri gönderimleri Vekil Sunucular, İçerik Taraması ve filtreleme, Anti-Virüs ve Anti-Malware Çözümleri, IPS/IDS Sistemleri, Güvenlik Duvarları ve bu sistemler için doğrulama dahil olmak üzere müşteri güvenlik ortamına tamamen uyar.

DCA'nın oluşturduğu ağ trafiği düşük seviyeye tutulur ve taranan IP adresi sayısına göre değişir. Aşağıdaki tablo DCA ile meydana gelen ağ yükü ile tekil standart internet sayfası ile meydana gelen ağ yükünü ana hatlarıyla göstermektedir.

Tek bir standart internet sayfasının yüklenmesi	60 K	(Yak. Top. Kbyte)
DCA taraması, boş IP	5 K	
DCA taraması, 1 yazıcı	7 K	
DCA taraması, 1 yazıcı, 1 alt-ağ	96 K	
DCA taraması, 13 yazıcıdan oluşan ağ	111 K	

Kullanılacak DCA'ların konum ve sayısı müşteri IT ağına göre değişir. Her bir DCA en fazla 2.000 cihazdan veri toplayabilir